Protected A

MEMORANDUM OF UNDERSTANDING ON INFORMATION SHARING

BETWEEN

DEPARTMENT OF CITIZENSHIP AND IMMIGRATION (herein referred to as "Immigration, Refugees and Citizenship Canada" or "IRCC")

And

THE ROYAL CANADIAN MOUNTED POLICE (herein referred to as "RCMP")

Collectively referred to as the "Participants"

1. PREAMBLE

1.1 The effective administration and enforcement of immigration, refugee, citizenship and passport law in Canada is important to: preserving the integrity of Canada's immigration, refugee, citizenship and passport programs and maintaining and protecting the health, safety and security of Canada. The partnership and strong corporate relations between IRCC and the RCMP are vital to ensuring the understanding and the effective administration and enforcement of the *Immigration and Refugee Protection Act* (IRPA), the *Citizenship Act*, the law of Canada respecting passports or other travel documents and other Acts of Parliament with provisions relating to immigration, refugees and citizenship matters.

2. MANDATES AND AUTHORITIES

2.1 Immigration, Refugees and Citizenship Canada is responsible for facilitating the arrival of people and their integration into Canada in a way that maximizes their contribution to the country while protecting the health, safety and security of Canadians. The Department also: maintains Canada's humanitarian tradition by protecting refugees and people in need of protection; promotes the rights and responsibilities of Canadian citizenship; facilitates international travel and entry to Canada for eligible Canadians, Permanent Residents and Protected Persons through the issuance of secure, globally recognized travel documents; and facilitates increased intercultural understanding to foster an integrated society with equal opportunity for all, regardless of race, ethnicity or religion. These objectives are achieved through the administration of the *IRPA*, the *Department of Citizenship and Immigration Act* the *Immigration and Refugee Protection Regulations*, the *Citizenship Act*, the law of Canada respecting passports or other travel documents and the *Citizenship Regulations*.

2.2 Under the authority of the *RCMP Act* and *RCMP Regulations* and common law powers, the RCMP enforces federal, provincial, and municipal laws, collects criminal intelligence, secures Canada's borders between official ports of entry and ensures the safety of major events, state officials, dignitaries and foreign missions. The RCMP is also charged with protecting Canada's institutions and national security by preserving public safety and the integrity of Canada's political and economic systems. Under its federal policing mandate, the RCMP investigates serious and organized crime, financial crime, and criminal activity related to national security. Legislated authority to conduct these investigations is derived from a number of acts; key among these are the *Criminal Code, Security Offences Act and Security of Information Act*. Within this context, the RCMP maintains, or has access to, national data repositories and national databases that include fingerprints, criminal records, the Canadian Police Information Centre (CPIC) and the Automated Criminal Intelligence Information System.

3. PURPOSE

3.1 The purpose of this Memorandum of Understanding (MOU) is to establish, in general terms, the basis for cooperation and coordination between the Participants, including their respective roles and responsibilities, as it relates to managing entry to Canada; preventing inadmissible persons from remaining in Canada and preventing prohibited individuals from acquiring Canadian citizenship or travel documents. This includes:

- information and intelligence sharing;
- ensuring information protection;
- effective communication;
- maintaining fingerprints for IRCC purposes within the national fingerprint repository;
- fingerprinting and screening, as required, of foreign nationals or permanent residents;
- developing, analyzing and distributing immigration and citizenship-related intelligence;
- investigating and, when appropriate, referring for prosecution offences contrary to the *IRPA, the* law if Canada respecting passports or other travel documents and the *Citizenship Act* and;
- supporting IRCC citizenship and civic engagement events such as: RCMP presence at citizenship ceremonies.

4. GOVERNANCE

4.1 The Participants will oversee their responsibilities under this MOU by means of a National Joint Committee (NJC). The NJC will be comprised of representatives of the RCMP and IRCC as follows:

a. Assistant Deputy Minister, Operations, IRCC
b. Executive Director, Strategic Policy and External Relations, Federal Policing, RCMP
c. Associate Assistant Deputy Minister, Operations, IRCC
d. Assistant Commissioner, Forensic Science and Identification Services, Specialized Policing Services, or delegate, RCMP
e. Director General, Integrity Risk Guidance Branch, IRCC
f. IRCC and RCMP representatives as identified by (a) and (d), including regional representatives.

4.2 The NJC will meet within three (3) months of the signing of this arrangement and no less than once every twelve (12) months thereafter, and more often if necessary. The NJC is charged with discussing programmatic, legal and policy issues as they relate to the terms set out in the MOU. The Participants' roles and responsibilities,

either joint or individual, are listed in the NJC's Terms of Reference.

5. PRINCIPLES

5.1 The Participants mutually accept the guiding principles of this arrangement, specifically:

a) striving for excellence in the working relationship between the Participants;
b) continuously seeking to improve relationship and client service through the effective use of human resources and technology, effective performance measurement, the use of service standards and accountability framework and risk management strategies;
c) as per the Terms of Reference, the NJC will review and evaluate the activities being carried out under the purview of the MOU; and
d) consulting each other in the development and implementation of policies, programs, operations or legislation that could affect cooperation between the Participants and the function of this MOU by identifying and reporting issues that may require mutual resolution.

6. FINANCIAL ARRANGEMENTS

6.1 Unless otherwise specified, both Participants will bear their respective costs incurred as a result of carrying out their respective responsibilities identified in this MOU and work cooperatively and supportively in assessing the financial implications that changes to Government policies or practices may have on their organization.

7. COLLECTION, USE, DISCLOSURE, RETENTION AND DISPOSITION OF INFORMATION

7.1 This section outlines the principles that will govern access, collection, use, disclosure, retention, and disposition of information including personal information by staff of the Participants for purposes related to this MOU.

7.2 Personal information will be used in a manner consistent with the reason for which it was collected unless otherwise provided by law. Procedures with respect to the collection, use, disclosure, retention and disposal of personal information will conform to the *Access to Information Act*, the *Privacy Act*, the *Library and Archives of Canada Act*, the Government of Canada Security Policy, the Treasury Board policies or directives on the sharing of personal information, *the Canadian Charter of Rights and Freedoms*, and any other applicable federal laws or policies relating to the management of information.

7.3 Each Participant will ensure that the appropriate security provisions are included in the annexes and any related appendices and that the standards and requirements of the Policy on Government Security and the Operational Standard for the *Security of Information Act* and any other applicable laws or policies are met.

7.4 The information received by the collecting Participant under this MOU will not be provided to a Third Party except where authorized or required by law.

7.5 Where a Participant is of the opinion that compliance with any of the provisions in this MOU and the accompanying annexes and appendices would likely be inconsistent with "Third Party" relationships, security, public policy, or other interests, it may either decline to provide the information and intelligence in whole or in part or offer to provide the information in whole or in part subject to such terms and conditions as it may specify. The Participant requesting the information or intelligence intend to comply with such terms and conditions as a condition precedent to its being provided.

7.6 In the event that a Participant receives a request under the *Privacy Act* or the *Access to Information Act* to disclose information supplied by the other Participant, it will notify the other Participant and process the request in accordance with the law.

7.7 Where either Participant is subject to a subpoena or other court order with regard to information supplied by the other Participant, the Participant in receipt of the subpoena or other court order will notify the other Participant as soon as possible, and provide details of the information to which it refers.

For the RCMP: Executive Director,
Federal Policing Strategic Policy and External Relations
73 Leikin Drive, Ottawa, Ontario

For IRCC: Director General
Immigration Program Guidance
365 Laurier Avenue West, Ottawa, Ontario

8. ACCURACY OF INFORMATION

8.1 Pursuant to Section 6(2) of the *Privacy Act* and in accordance with the MOU, each Participant will take all reasonable steps to ensure the completeness, accuracy and timeliness of the personal information.

8.2 Each Participant will notify the other, in writing within a reasonable time, if it becomes aware that the information shared is not accurate, complete, and up-to-date, and will take all reasonably available steps to amend the information.

8.3 Each Participant intends, with respect to Personal Information that is under their control, to respond to requests from individuals to access and correct their Personal Information. Each Participant intends to notify the other Participant of the request and the corrected information. Each Participant also intends to respect each other's revisions to the information.

8.4 Information may not be edited, or otherwise modified unless directed or authorized by the Participant providing the information.

9. PRIVACY BREACH

9.1 The Participants intend to follow the *TBS Guidelines for Privacy Breaches* as well as the processes established by their respective legislation, policies, and guidelines in order to ensure there are no Privacy Breaches.

9.2 A Participant becoming aware of a Privacy Breach will:

a) follow the processes established by its policies to manage and respond to Privacy Breaches;
b) immediately notify the other Participant and provide details regarding the circumstances of the Privacy Breach; and
c) investigate the Privacy Breach and report its findings and any remedial actions taken to the other Participant within a reasonable time.

9.3 A Participant notified of a Privacy Breach may:

a) review the steps taken or proposed by the other Participant to address the Privacy Breach and prevent a recurrence of it;
b) request the other Participant take specific steps to address the Privacy Breach or prevent a recurrence of it;
c) suspend the sharing of information until satisfied that the other Participant has complied with the provisions of this MOU. The Participant will advise the other if considering this course of action.

9.4 If the Participants disagree on the steps to be taken to mitigate the consequences of, or prevent recurrence of, a Privacy Breach, the Participants will follow the Dispute Resolution of this MOU.

10. ANNEXES AND SUB-ARRANGEMENTS

10.1 The Annexes and Appendices comprise an integral part of this MOU and carry the full force and effect of any other part of this MOU.

10.2 Signatories for each Annex will be designated by the Participants in accordance with

the subject matter in each Annex.

10.3 New Annexes and/or sub-arrangements may be developed as required at any time with the approval of the NJC. Such arrangements will be consistent with the provisions set out in this MOU and, in the case of a dispute, the national MOU will take precedence.

10.4 Both Participants will retain signed original copies of these arrangements for inclusion in their respective information management repositories.

10.5 As the passport functions continue to be integrated in IRCC over time, any relevant pre-existing passport arrangements or agreements and subsidiary activity will be progressively integrated within the scope and framework of this MOU.

11. DISPUTE RESOLUTION

11.1 In the event of a dispute arising from the interpretation or operation of this MOU, including the attached Annexes, the Participants will endeavor to jointly resolve the matter at the lowest administrative level possible. In the event a resolution is not reached at the lowest possible level, the matter will be referred to the next level up until there is resolution. In the event of a failure to resolve a disagreement at the level of the NJC, the Participants will refer the matter to the signatories of this arrangement.

12. LIABILITY

12.1 The RCMP will assume any and all costs, damages or awards imposed against the RCMP where the RCMP or its representative was negligent or reckless in its actions, pursuant to this MOU. Save and except where the RCMP was negligent or reckless in its actions, IRCC will reimburse the RCMP for any and all costs, damages and awards imposed against the RCMP which occurred as a result of the RCMP's participation in this MOU.

13. AMENDMENTS

13.1 This MOU and its related annexes and any appendices may be amended at any time, with the mutual consent of the Participants.

13.2 An amendment to this MOU must be in writing and signed by the signatories to this MOU.

13.3 Amendments to an Annex or appendix must be in writing and signed by the signatories of the Annex or appendix. Amendments to the Annex or appendix

may not change the intent and scope of this MOU without the consent of the MOU signatories.

13.4 Both Participants intend to notify each other in writing should any regulatory, legislative or policy changes likely affect this MOU.

14. APPLICATION AND DURATION

14.1 This MOU will come into force when signed by the last of the Participants. Annexes and appendices to this MOU are effective from their date of signing by both Participants.

14.2 This MOU repeals and replaces the 2012 MOU. Annexes signed in 2012 will remain in effect, as integral part of this MOU, until replaced or amended.

14.3 This MOU and its annexes are subject to a review every five years and the first review will commence five years from the date of signing, or by mutual acceptance of the two signatories.

15. TERMINATION

15.1 This MOU can be terminated in one of the following ways:

a) at any time by written acceptance of the Participants; or

b) by either Participant's signatory by providing at least three (3) months' notice in writing; or

c) by either Participant at any time if a Participant fails to meet its obligations under this MOU, and having followed the dispute prevention and resolution provisions in Section 11.

15.2 The Participants understand that their responsibilities to protect and maintain the integrity of the information shared under this MOU, including retention and disposition of the information, continue after this MOU is terminated.

16. SIGNATURES

IN WITNESS THEREOF, this Memorandum of Understanding, in both official languages, was signed in duplicate, each copy being equally authentic.

For Immigration, Refugees and Citizenship Canada:

Marta Morgan
Deputy Minister, IRCC

JUN 7 - 2017
Date

For the Royal Canadian Mounted Police:

Bob Paulson
The Commissioner of the RCMP

MAY 0 7 2017
Date

Protégé A

PROTOCOLE D'ENTENTE SUR L'ÉCHANGE D'INFORMATION

ENTRE

LE MINISTÈRE DE LA CITOYENNETÉ ET DE L'IMMIGRATION (ci-après nommé « Immigration, Réfugiés et Citoyenneté Canada » ou « IRCC »)

et

LA GENDARMERIE ROYALE DU CANADA (ci-après nommée la « GRC »).

Collectivement appelés les « participants »

1. PRÉAMBULE

1.1 L'application et l'exécution efficaces des lois sur l'immigration, les réfugiés, la citoyenneté et les passeports au Canada sont importantes pour préserver l'intégrité des programmes d'immigration, des réfugiés, de la citoyenneté et des passeports du Canada et pour maintenir et protéger la santé ainsi que la sécurité des Canadiens. Le partenariat et les liens organisationnels solides entre IRCC et la GRC sont essentiels pour assurer la compréhension ainsi que l'administration et l'application efficaces de la *Loi sur l'immigration et la protection des réfugiés* (LIPR), de la *Loi sur la citoyenneté*, de la loi du Canada en matière de passeports ou des autres documents de voyage, ainsi que de toute autre loi du Parlement comprenant des dispositions relatives à l'immigration, aux réfugiés et à la citoyenneté.

2. LES MANDATS ET LES POUVOIRS

2.1 Il incombe à IRCC de faciliter l'arrivée des personnes et leur intégration au Canada de manière à optimiser leur apport au pays tout en protégeant la santé des Canadiens et en assurant leur sécurité. Le Ministère doit aussi : maintenir la tradition humanitaire du Canada en protégeant les réfugiés et les personnes ayant besoin de protection; promouvoir les droits et les responsabilités rattachés à la citoyenneté canadienne; faciliter les voyages internationaux et l'entrée au Canada pour les Canadiens, les résidents permanents et les personnes protégées admissibles en délivrant des documents de voyage sécurisés et reconnus à l'échelle mondiale; et accroître la compréhension interculturelle afin de permettre le maintien d'une société intégrée qui offre des chances égales à tous, peu importe la race, l'origine ethnique ou la religion. Ces objectifs sont atteints grâce à l'administration de la *LIPR*, de la *Loi sur le ministère de la Citoyenneté et de l'Immigration*, du *Règlement sur l'immigration et la protection des réfugiés*, de la *Loi sur la citoyenneté*, des lois du Canada régissant les passeports ou tout autre document de voyage, ainsi que du *Règlement sur la citoyenneté*.

2.2 Aux termes de la *Loi sur la GRC* et du *Règlement sur la GRC*, ainsi que des pouvoirs conférés par la common law, la GRC applique la législation et la réglementation fédérales, provinciales et municipales, recueille des renseignements sur les activités criminelles, sécurise les frontières du Canada entre les points d'entrée officiels et assure la sécurité lors d'événements majeurs et pour les représentants de l'État, les dignitaires et les missions étrangères. Il incombe également à la GRC de protéger les institutions du Canada et d'assurer la sécurité nationale en protégeant le public et en préservant l'intégrité des systèmes politiques et économiques du Canada. En vertu de son mandat de police fédérale, la GRC enquête sur les crimes graves et les activités liées au crime organisé, les crimes économiques et les activités criminelles rattachées à la sécurité nationale. Un certain nombre de lois confèrent à la GRC le pouvoir de mener ces enquêtes, notamment le Code criminel, la *Loi sur les*

infractions en matière de sécurité et la *Loi sur la protection de l'information*. C'est dans ce contexte que la GRC tient et consulte des bases de données et des dépôts nationaux qui contiennent, entre autres, des empreintes digitales et des casiers judiciaires, et elle a accès au Centre d'information de la police canadienne (CIPC) et au Système automatisé de renseignements sur la criminalité (SARC).

3. OBJET

3.1 Le présent protocole d'entente (PE) vise à établir, en termes généraux, le fondement de la coopération et de la coordination entre les participants, y compris leurs rôles et responsabilités respectifs pour ce qui est de gérer l'entrée au Canada, d'empêcher les personnes non admissibles à demeurer au Canada, et d'empêcher les personnes interdites au Canada d'obtenir la citoyenneté canadienne ou des documents de voyage. Cela comprend :

- la communication de l'information et du renseignement;
- le maintien de la protection des renseignements;
- la communication efficace;
- la tenue, pour les besoins d'IRCC, d'empreintes digitales dans le dépôt national d'empreintes digitales;
- la dactyloscopie et le filtrage, au besoin, d'étrangers ou de résidents permanents;
- l'établissement, l'analyse et la diffusion de renseignements en matière d'immigration et de citoyenneté;
- la réalisation d'enquêtes et, au besoin, le renvoi de cas devant faire l'objet de poursuites relativement à des infractions à la *LIPR*, aux lois du Canada en matière de passeports ou d'autres documents de voyage et à la *Loi sur la citoyenneté*;
- le soutien des activités de citoyenneté et d'engagement civique d'IRCC comme la présence de la GRC aux cérémonies de citoyenneté.

4. GOUVERNANCE

4.1 Un Conseil national mixte (CNM) supervisera les responsabilités attribuées aux participants en vertu du présent PE. Le CNM est composé de représentants de la GRC et d'IRCC :

a. sous-ministre adjoint, Opérations, IRCC;
b. directeur exécutif, Direction des politiques stratégiques et des relations extérieures, Police fédérale, GRC;
c. sous-ministre adjoint délégué, Opérations, IRCC;
d. commissaire adjoint, Services des sciences judiciaires et de l'identité, Services de police spécialisés, ou délégué, GRC;
e. directeur général, Direction générale de l'orientation sur les risques, IRCC;
f. représentants d'IRCC et de la GRC désignés par les titulaires des postes indiqués aux puces (a) et (d), y compris des représentants des régions.

4.2 Le CNM tiendra des réunions dans les trois (3) mois suivant la signature du protocole, au moins tous les douze (12) mois par la suite et plus fréquemment au besoin. Il incombe au CNM d'examiner les enjeux liés aux programmes, aux lois et aux stratégies dans la mesure où ils se rapportent aux termes du PE. Les rôles et responsabilités des participants, qu'ils soient communs ou individuels, sont énumérés dans le mandat du CNM.

5. PRINCIPES

5.1 Les participants conviennent mutuellement des principes directeurs de la présente entente, soit :

a) viser l'excellence dans les relations de travail entre les participants;
b) chercher continuellement à améliorer le partenariat et les services aux clients, en utilisant efficacement les ressources humaines et la technologie, en mesurant efficacement le rendement et en faisant appel à des normes de service, à un cadre de responsabilisation et à des stratégies de gestion du risque;
c) conformément au mandat, examiner et évaluer (CNM) les activités menées relevant du PE;
d) se consulter mutuellement pour élaborer et mettre en œuvre des politiques, des programmes, des activités ou des lois qui pourraient avoir une incidence sur la collaboration entre les participants et la fonction du présent PE, et signaler les enjeux pouvant nécessiter une résolution mutuelle.

6. DISPOSITIONS FINANCIÈRES

6.1 Sauf indication contraire, les deux participants assument les coûts respectifs engagés en conséquence de l'exécution de leurs responsabilités respectives dans le cadre du présent PE et ils travaillent de façon coopérative et constructive lorsqu'ils évaluent les incidences financières que les changements apportés aux politiques ou aux pratiques du gouvernement peuvent avoir sur leur organisme.

7. COLLECTE, UTILISATION, DIVULGATION, CONSERVATION ET ÉLIMINATION DES RENSEIGNEMENTS

7.1 Cette section présente les principes qui régiront la collecte, l'utilisation, la communication, la conservation et l'élimination des renseignements, y compris les renseignements personnels, par le personnel des participants, et ce, à des fins liées au présent PE.

7.2 Les renseignements personnels sont utilisés conformément aux fins auxquelles ils ont été recueillis, sauf disposition législative contraire. Les procédures de collecte,

d'utilisation, de divulgation, de conservation et d'élimination des renseignements personnels doivent être conformes à la *Loi sur l'accès à l'information*, à la *Loi sur la protection des renseignements personnels*, à la *Loi sur la Bibliothèque et les Archives du Canada*, à la Politique sur la sécurité du gouvernement du Canada, aux politiques ou aux directives du Conseil du Trésor sur l'échange de renseignements personnels, à la Charte canadienne des droits et libertés et à toutes les autres lois et politiques fédérales applicables à la gestion de l'information.

7.3 Chaque participant veille à ce que les dispositions de sécurité appropriées soient incluses dans les annexes et tous les appendices connexes. Il veille aussi à ce que les normes et exigences de la Politique sur la sécurité du gouvernement et à ce que la norme opérationnelle de la *Loi sur la protection de l'information* et toutes les autres lois ou politiques applicables soient respectées.

7.4 Le participant qui reçoit des renseignements en vertu du présent PE ne les transmet pas à un tiers, à moins que la loi l'autorise ou l'exige.

7.5 Si un participant estime que l'application de toute disposition du présent PE et de ses annexes et appendices risque de compromettre des liens avec des tiers, la sécurité, l'intérêt public ou d'autres intérêts, il peut refuser de fournir la totalité ou une partie des renseignements ou accepter d'en fournir une partie ou la totalité, sous réserve des conditions qu'il juge bon d'imposer. Le participant qui demande de l'information ou des renseignements a l'intention de se conformer auxdites modalités avant que l'information ou les renseignements soient fournis.

7.6 Si un participant reçoit une demande aux termes de la *Loi sur la protection des renseignements personnels* ou de la *Loi sur l'accès à l'information* pour la divulgation d'information fournie par l'autre participant, il doit en aviser l'autre participant et traiter la demande conformément à la loi.

7.7 Lorsque l'un ou l'autre des participants est assigné à comparaître ou soumis à quelque autre ordonnance d'un tribunal concernant de l'information fournie par l'autre participant, le participant assigné à comparaître ou soumis à l'ordonnance du tribunal doit en aviser l'autre immédiatement et lui fournir des précisions sur l'information en question.

Pour la GRC : Directeur exécutif
Direction des politiques stratégiques et des relations extérieures
73, promenade Leikin, Ottawa (Ontario)

Pour IRCC : Directeur général
Direction générale de l'orientation du programme d'immigration
365, avenue Laurier Ouest, Ottawa (Ontario)

8. EXACTITUDE DES RENSEIGNEMENTS

8.1 Conformément au paragraphe 6(2) de la *Loi sur la protection des renseignements personnels*, et en conformité du PE, chaque participant doit prendre toutes les mesures raisonnables pour veiller à ce que les renseignements personnels soient complets, exacts et à jour.

8.2 Chaque participant doit aviser l'autre, par écrit et dans un délai raisonnable, s'il se rend compte que les renseignements échangés ne sont pas exacts, complets ou à jour, et il doit prendre toutes les mesures raisonnablement mises à sa disposition pour modifier lesdits renseignements.

8.3 Chaque participant a l'intention, en ce qui concerne les renseignements personnels qui sont sous son contrôle, de répondre aux demandes de personnes qui souhaitent accéder à leurs renseignements personnels et les corriger. Chaque participant a l'intention d'informer l'autre lorsqu'il répond à de telles demandes ou apporte des corrections. Chaque participant a également l'intention de respecter les révisions de l'information apportées par l'autre.

8.4 Les renseignements ne peuvent pas être modifiés ou autrement altérés, à moins que le participant qui les fournit ne donne des directives ou n'accorde une autorisation par écrit en ce sens.

9. ATTEINTE À LA VIE PRIVÉE

9.1 Les participants ont l'intention de respecter les Lignes directrices sur les atteintes à la vie privée du Secrétariat du Conseil du Trésor (SCT) ainsi que les processus établis dans le cadre de leurs politiques, législation et lignes directrices respectives pour veiller à ce qu'il n'y ait pas d'atteintes à la vie privée.

9.2 Un participant qui est mis au fait d'une atteinte à la vie privée doit :

a) suivre les processus établis par ses politiques afin de gérer cette atteinte à la vie privée et d'y donner suite;
b) aviser immédiatement l'autre participant et fournir des détails sur les circonstances entourant l'atteinte à la vie privée;
c) enquêter sur l'atteinte à la vie privée et présenter à l'autre participant, dans un délai raisonnable, ses conclusions et les mesures correctives prises.

9.3 Un participant informé d'une atteinte à la vie privée peut :

a) examiner les mesures prises ou proposées par l'autre participant en vue de remédier à l'atteinte à la vie privée et d'empêcher qu'elle ne se reproduise;

b) demander à l'autre participant de prendre des mesures particulières pour remédier à l'atteinte à la vie privée ou empêcher qu'elle ne se reproduise;
c) suspendre l'échange de renseignements tant qu'il ne sera pas satisfait que l'autre participant s'est conformé aux dispositions du présent PE. Le participant doit informer l'autre participant s'il envisage de recourir à cette mesure.

9.4 Si les participants ne s'entendent pas sur les mesures à prendre pour atténuer les conséquences d'une atteinte à la vie privée ou empêcher qu'une telle atteinte ne se reproduise, ils doivent suivre le processus de règlement des différends du présent PE.

10. ANNEXES ET SOUS-ARRANGEMENTS

10.1 Les annexes et appendices font partie intégrante du présent PE et prennent effet comme toute autre partie du présent PE.

10.2 Les signataires pour chaque annexe sont désignés par les participants, conformément aux questions traitées dans chaque annexe.

10.3 De nouvelles annexes ou nouveaux sous-arrangements peuvent être rédigés au besoin et en tout temps, avec l'approbation du CNM. Lesdits arrangements doivent être conformes aux dispositions stipulées dans le présent PE. En cas de différend, le PE national prévaudra.

10.4 Les deux participants conservent des exemplaires originaux signés desdits arrangements pour qu'ils soient inclus dans leurs dépôts respectifs de gestion de l'information.

10.5 À mesure que les fonctions rattachées aux passeports continueront d'être intégrées aux fonctions d'IRCC, tous les arrangements ou accords préexistants pertinents sur les passeports, ainsi que toutes les activités secondaires, seront progressivement intégrés, dans les limites de la portée et du cadre du présent PE.

11. RÈGLEMENT DES DIFFÉRENDS

11.1 Advenant un différend sur l'interprétation ou le fonctionnement du présent PE, y compris les annexes, les participants s'efforcent de régler conjointement le différend à l'échelon administratif le plus bas possible. Si on ne peut régler le différend au plus bas niveau possible, la question est transmise à l'échelon supérieur jusqu'à sa résolution. Si, une fois l'échelon du CNM atteint, celui-ci ne parvient pas à résoudre le différend, les participants renvoient l'affaire aux signataires de la présente entente.

12. RESPONSABILITÉ

12.1 La GRC assume tous les coûts, dommages-intérêts ou indemnisations qui lui sont imposés dans les cas où elle, ou son représentant, a fait preuve d'insouciance ou de négligence dans ses actes, aux termes du présent PE. Sauf dans les cas où la GRC a fait preuve d'insouciance ou de négligence, IRCC rembourse à la GRC tous les coûts, dommages-intérêts ou indemnisations qui lui sont imposés par suite de sa participation au présent PE.

13. MODIFICATIONS

13.1 Le présent PE, les annexes qui s'y rattachent ainsi que tout appendice peuvent être modifiés en tout temps, avec le consentement mutuel des participants.

13.2 Toute modification au présent PE doit être apportée par écrit et signée par les signataires du protocole.

13.3 Les modifications à une annexe ou à un appendice doivent être apportées par écrit et être signées par les signataires de l'annexe ou de l'appendice. Les modifications à une annexe ou à un appendice ne peuvent pas modifier l'objectif ou la portée du présent PE sans le consentement des signataires du PE.

13.4 Les deux participants conviennent de s'informer mutuellement par écrit de tout changement réglementaire, législatif ou politique pouvant influencer le présent PE.

14. APPLICATION ET DURÉE

14.1 Le présent PE entre en vigueur dès sa signature par le dernier des participants. Les annexes et appendices au présent PE sont en vigueur à compter de la date de leur signature par les deux parties.

14.2 Le présent PE annule et remplace le PE de 2012. Les annexes signées en 2012 demeurent en vigueur en tant que partie intégrante du présent PE, jusqu'à ce qu'elles soient remplacées ou modifiées.

14.3 Le présent PE et ses annexes font l'objet d'un examen tous les cinq ans, et le premier examen a lieu cinq ans après la date de la signature ou à la date qui convient aux deux signataires.

15. RÉSILIATION

15.1 Le présent PE peut être résilié de l'une des façons suivantes :

a) à tout moment si les participants en conviennent par écrit;

b) par la signature d'un participant qui signifie à l'autre un avis écrit d'au moins trois (3) mois;

c) par un participant à tout moment si l'un des participants omet de respecter ses obligations prévues dans le présent PE et après avoir suivi le processus de prévention et de règlement des différends décrit à la section 11.

15.2 Les participants comprennent que leurs responsabilités liées à la protection et au maintien de l'intégrité des renseignements échangés en vertu du présent PE, y compris la conservation et l'élimination des renseignements, se poursuivent après la résiliation du présent PE.

16. SIGNATURES

EN FOI DE QUOI, le présent Protocole d'entente, rédigé dans les deux langues officielles, est signé en double exemplaire, chaque copie faisant également foi.

Pour Immigration, Réfugiés et Citoyenneté Canada

Marta Morgan
Sous-ministre, IRCC

JUN 7 - 2017
Date

Pour la Gendarmerie royale du Canada :

Bob Paulson
Commissaire de la GRC

MAR 3 1 2017
Date

MEMORANDUM OF UNDERSTANDING BETWEEN THE DEPARTMENT OF CITIZENSHIP AND IMMIGRATION (herein referred to as "Immigration, Refugees and Citizenship Canada" or "IRCC") AND THE ROYAL CANADIAN MOUNTED POLICE (herein referred to as "RCMP"). Collectively referred to as the Participants

ANNEX I: Disclosing and collecting personal information held by the RCMP's Canadian Criminal Real Time Identification Services (CCRTIS) Systems for the purposes of screening immigration and citizenship applicants

1. BACKGROUND

Immigration, Refugees and Citizenship Canada (IRCC) is authorized, under the *Immigration and Refugee Protection Act* (IRPA), the *Citizenship Act* and their respective regulations, to take the necessary steps to prevent persons who are inadmissible pursuant to the provisions of the IRPA from entering or remaining in Canada as well as to ensure that prohibited individuals do not acquire citizenship.

The Royal Canadian Mounted Police (RCMP) is in possession of personal information, under the *Criminal Records Act*, the *Youth Criminal Justice Act* and the *Immigration Refugee Protection Act*, held by the Canadian Criminal Real Time Identification Services' (CCRTIS) Systems. The CCRTIS maintains the national repository of criminal record information, which includes fingerprints, and is mandated to provide direct operational support to the Canadian law enforcement, criminal justice and public security communities for criminal, civil and immigration purposes. This personal information may be relevant to IRCC for the purpose of establishing identity and verifying whether an applicant meets the requirements for eligibility and admissibility as it relates to criminality under the IRPA or eligibility under the *Citizenship Act*.

Canadian Criminal Real Time Identification Service is also the national provider of biometric-based criminal record verifications for civil and criminal court purposes, the security screening environment for all levels of government and the general public.

The Participants desire to work together to prevent persons who are inadmissible to Canada from entering or remaining in Canada and prevent individuals who are ineligible from acquiring Canadian citizenship.

2. PURPOSE AND SCOPE

2.1 The purpose of this Annex is to set out the roles and responsibilities of the Participants as they apply to screening and the sharing of personal information of IRCC clients.

2.2 For the purposes of this Annex, IRCC provides personal information to the RCMP, pursuant to section 8(2)(a) of the *Privacy Act*, who then responds to the request based on releasable information contained in CCRTIS databases. This information is used for the

purpose of determining admissibility and/or eligibility of individuals under the IRPA, its regulations and/or the *Citizenship Act* as well as identity management. Details of the information that IRCC will provide to the RCMP, as well as the response from the RCMP, are included in Appendix A.

2.3 For the RCMP, the scope of the personal information covered by this Annex, and its sharing, is limited to the information held by the RCMP's CCRTIS Systems.

3. DEFINITIONS

3.1 For the purposes of this Annex, terms which are defined in the IRPA, the Immigration and Refugee Protection Regulations, *the Citizenship Act*, the Citizenship Regulations or in the Criminal Code, keep the same meaning. The following terms have the meaning identified below:

a) Biometric information: means the fingerprints and photographs of a foreign national or a permanent resident.
b) "Designated Representatives" are the primary contacts for the Participants responsible for monitoring the implementation of this Annex. This includes the interpretation, inquiries and requests for amendments of this Annex and addressing any issues that arise from it, including compliance with the provisions.
c) "Dispute" means a conflict or disagreement respecting:
    i. the interpretation, application, or implementation of this Annex; or
    ii. non-compliance or anticipated non-compliance with this Annex.
d) "Personal Information" means information about an identifiable individual that is recorded in any form as defined in Section 3 of the *Privacy Act*.
e) "Privacy Breach" is the unauthorized collection, use, disclosure, access, storage or disposal of Personal Information, whether deliberate or accidental.
f) Record suspension: means the suspension of a criminal record as defined in 2(1) of the *Criminal Record Act*.
g) Screening: refers to the determination of admissibility and eligibility by IRCC via the sharing of personal information held by the RCMP, specifically by the Real Time Identification system (RTID).

4. RESPONSIBILITIES OF IRCC

4.1 Assess the information provided by the RCMP to determine admissibility under IRPA and its related Regulations and eligibility of individuals under the Citizenship Act.

4.2 Respect caveats placed on personal information regarding its use, classification or further dissemination.

4.3 Understand that the accuracy of fingerprint searches by the RCMP is dependent on the quality of fingerprints.

4.4 Amend and purge an individual's personal information held by the RCMP in the immigration repositories on IRCC's behalf.

4.5 Ensure that the immigration information of individuals who become Canadian citizens is removed from the RCMP system in a mutually acceptable timeframe to the Participants.

4.6 Assume the risk that individuals' personal information may be released to law enforcement partners in the period between becoming a citizen and the purging of their immigration information when authorized by law.

5. RESPONSIBILITIES OF THE RCMP

5.1 Support IRCC by conducting searches of the criminal and immigration databases held by the CCRTIS and provide IRCC with the results of those searches.

5.2 Provide IRCC with appropriate certified documents upon request, and where relevant (e.g., for the purposes of prohibition cases).

5.3 Subsequent to a name-based IRCC screening request, make all reasonable efforts to provide criminal record information that is releasable by the RCMP on known IRCC subjects to IRCC in a mutually acceptable timeframe to the Participants.

5.4 Subsequent to a biometric-based IRCC screening request, make all reasonable efforts to provide criminal record information as well as immigration information that is releasable by the RCMP on known IRCC subjects to IRCC in a mutually acceptable timeframe to the Participants.

5.5 Respect caveats and limitations placed on personal information regarding its use, classification, handling and/or further dissemination. In the case of information received from a Five Country Conference partner or another international partner, caveats and limitations imposed by that partner will also apply.

5.6 Notify IRCC of the record suspension if Canadian criminal information was disclosed to IRCC and the RCMP subsequently becomes aware that a record suspension was granted for charges against an individual.

5.7 Send a system error response to IRCC when fingerprints do not meet the quality threshold of the Automated Fingerprint Identification System (AFIS) (i.e., submission rejected). The RCMP will perform a quality assurance function by manually reviewing a mutually accepted percentage of fingerprints rejected by the CCRTIS, and will inform IRCC of the reasons why the transactions could not be processed.

5.8

6. JOINT RESPONSIBILITIES OF THE PARTICIPANTS

6.1 When required, the Participants will consult each other prior to any changes resulting from Government of Canada policy or legislative amendments, or commitments that may impact transaction volumes, special programs or other items within this Annex. The Participants acknowledge that sufficient funding will be considered before any volume changes or new programs are implemented.

6.2 In collaboration and subject to IRPA and the *Citizenship Act*, the Participants will determine the personal information necessary for IRCC to determine admissibility and/or eligibility of individuals. A separate matrix has been developed to outline each of the processes, the related elements of personal information that IRCC provides to the RCMP and the data results that are provided by the RCMP (see Appendix "A"). The matrix will be updated as required and reviewed as part of the Annex.

6.3 The Participants will notify one another immediately of any unplanned/unexpected system outages that will affect biographic and biometric transactions.

7. RETENTION, USE AND DISPOSAL OF INFORMATION

7.1 The Participants understand that the retention and disposal period of the biometric information collected by IRCC is set by IRCC. IRCC will retain and dispose of all screening results provided by the RCMP's CCRTIS Systems, in accordance with the applicable Retention and Disposition schedule and as required under the *Privacy Act*, the *Library and Archives of Canada Act*, the *Criminal Records Act* and government policy.

7.2 As per this Annex, unless permitted or required by law, the personal information shared and retained between the Participants for the purpose of carrying out screening functions outlined in this Annex will not be used, disclosed or retained for any other purposes other than for which it was collected or created.

8. TRANSMISSION OF INFORMATION

8.1 The information covered in this Annex (Appendix "A") will be securely transmitted between the Participants in a manner conforming to their respective legislation, policies and directives for the secure transfer of information.

8.2 The Participants will take all available reasonable steps to reduce the risk of sharing harmful viruses, programs or data in the transmitted information. The Participants will

not be held responsible for any damage resulting from the transmission of harmful viruses, programs or data.

9. SECURITY OF INFORMATION

9.1 Each Participant will identify the security classification of information it discloses under this Annex and will treat all information received under this Annex in accordance with the security markings on it and with the security classification standards of the Government of Canada.

9.2 The Participants will ensure that only those employees whose duties require such access, will have access to the information supplied by each organization and that these employees have the necessary security clearance.

10. DESIGNATED REPRESENTATIVES:

10.1 Designated Representatives are the primary contacts for the Participants responsible for monitoring the implementation of this Annex. This includes the interpretation, inquiries, requests for amendments of this Annex and addressing any issues that arise from it.

10.2 For the purposes of this Annex, the following officials are the Designated Representatives:

For the RCMP: Director General,
Canadian Criminal Real Time Identification Services
1200 Vanier Parkway, Ottawa, Ontario

For IRCC: Director General,
Immigration Program Guidance
365 Laurier Avenue West, Ottawa, Ontario

Director General,
Integrity Risk Guidance Branch (IRG)
70 Crémazie Street, Gatineau, Quebec

10.3 Notices under this Annex will be in writing and delivered to the other Participant via the Designated Representative.

11. DISPUTE PREVENTION AND RESOLUTION

11.1 The Participants acknowledge making every reasonable effort to prevent a dispute arising from the interpretation or operation of this Annex. In the event of a dispute, the Participants will endeavor to jointly resolve the matter at the lowest administrative level

possible.

11.2 In the event a dispute cannot be resolved amicably, the Participants will escalate the matter in accordance with the procedures set out in the MOU for dispute resolution.

12. MONITORING

12.1 The Participants will review the practices and procedures outlined in this Annex to ensure that the provisions of the MOU are kept up-to-date, on the 5 year anniversary of its signing and every 5 year anniversary forthwith.

12.2 To reflect any changes resulting from the Biometrics Expansion Project, the Participants will review this Annex starting in May 2017 with a completion date of November 2017.

12.3 Each Participant will notify the other Participant in the event that any terms of this Annex are not respected.

13. TERMINATION

13.1 This Annex can be terminated in one of the following ways:

a) at any time by written acceptance of the Participants;
b) by either Participant's signatory by providing at least three (3) months' notice in writing; or
c) by either Participant at any time if a Participant fails to meet its obligations under this annex or MOU, and having followed the dispute prevention and resolution provisions in Section 11 of the annex.

13.2 The Participants acknowledge that their responsibilities to protect and maintain the integrity of the information shared under this Annex, including retention and disposal of the information, continue after this Annex is terminated.

14. AMENDMENTS

14.1 This Annex may be amended at any time by mutual consent, in writing, of the Participants.

15. ENTIRE UNDERSTANDING

15.1 This Annex and its Appendix represent the entire understanding between the Participants in relation to the screening function provided by the RCMP's CCRTIS and supersede the Screening Annex signed by the Participants in 2012 and the Biometrics Business Level Agreement signed in 2015.

16. FINANCIAL ARRANGEMENTS

16.1 The Participants will bear their own costs when exchanging information under this Annex. The Participants will absorb all incremental costs associated with the operation of this Annex.

16.2 The Participants acknowledge that each will bear its own costs in performing their respective activities and responsibilities under this Annex.

17. EFFECTIVE DATE

17.1 This Annex will become effective on the date it is signed by the last of the signatories and remain in effect until terminated in accordance with the procedures set out in this Annex.

18. SIGNATURES

IN WITNESS THEREOF, this Annex was signed in duplicate, each copy being equally authentic.

For Immigration, Refugees and Citizenship Canada:

M. M. [signature] — July 13/17.

Director General,
Immigration Program Guidance
365 Laurier Avenue West, Ottawa, Ontario

Date

[signature] — July 14/17

Director General,
Integrity Risk Guidance Branch (IRG)
70 Crémazie Street, Gatineau, Quebec

Date

For the Royal Canadian Mounted Police:

[signature] — 2017-06-15

Director General,
Canadian Criminal Real Time
Identification Services, RCMP

Date

Blank Page

Screening Category	Transaction type	Screening Authority	Personal Information	RCMP Screening Process	Retention and Disposition	Service Level Agreement	RCMP Screening Results
Biometric Screening of Temporary Residents (TR) Applicants from 29 countries and one territory, as prescribed in the *IRPR* Biometric screening of TR Applicants (s. 16(2) of the *IRPA*)	IMM	s.36 IRPA R 12.1	**Biometric:** Fingerprints and related biographic information as stipulated in the current RCMP NPS-NIST Interface Control document	CCRTIS will screen resulting fingerprint submissions against its national repository (containing criminal and immigration fingerprints).	Retained in the RCMP Immigration Database for 15 years from the date of biometric collection unless amended or obtains citizenship.	3 Business Days	Biometric screening results include a file number that corresponds to either a new or existing immigration file. Where available, an existing refugee file number, or a criminal/FPS number will be provided. Additional Information can be obtained through CPIC by IRCC.
Asylum Claimants and Overseas Refugee Resettlement Applicants	IMM	s.36 IRPA s.16(2) IRPA	Fingerprints and related biographic information as stipulated in the current RCMP NPS-NIST Interface Control document	CCRTIS will screen resulting fingerprint submissions against its national repository (containing criminal and immigration fingerprints).	Retained in the RCMP Immigration Database until the client reaches the age of 100 years, or obtains citizenship.	3 Business Days	CCRTIS will screen fingerprint submissions against its national fingerprint repository (containing criminal and immigration fingerprints) response details are stipulated in the current RCMP NPS-NIST Interface Control document.
Biographic Screening of PR Applicants: In-Canada	Name Based Search (NBS) /MAP	s.36	**Biographic:** Name, date of birth (if there is a possible name/date of birth match	**Systematic:** CPIC/CNI biographic check	Not Retained.	Name Search: 3 business days Fingerprint	Name Based – CCRTIS will provide a response of either No record or Inconclusive. An Inconclusive response requires the submission of a full set of

			for a client, client is requested to submit fingerprints) **Biometric:** Fingerprints and related biographic information as stipulated in the current RCMP NPS-NIST Interface Control document **(Civil Submission)**	**Case by case:** Fingerprints required when name match is inconclusive CCRTIS will screen resulting fingerprint submissions against its national repository (containing criminal and immigration fingerprints).		Search – 120 Days	fingerprints by the client utilizing the appropriate Application Type as defined by the RCMP. CCRTIS will screen fingerprint submissions against its national fingerprint repository (containing criminal and immigration fingerprints) response details are stipulated in the current RCMP NPS-NIST Interface Control document. The exact detail of the information that is disclosed is subject to legislative requirement and business rules and varies depending on the type of submission and the results of the search. Should the information be deemed releasable, the following information is released as a paper product, either to the client, who then forwards the results to IRCC or to IRCC directly. **Match to Refugee or TRB:** Biographic information included in the civil submission along with IRCC unique biometric ID and RCMP ID. **Match to Criminal:** Copy of certified criminal record as

							maintained in the central repository by the RCMP– subject to release of information rules.
Citizenship Applicants	Name Search/MAP	s. 36 IRPA Sec 21 & Sec 22 *Citizenship Act*	**Biographic:** Name, date of birth If there is a possible name match for a client, client is requested to submit fingerprints directly to the RCMP	**Systematic:** CPIC/CNI biographic check **Case by Case:** Fingerprints required when name match is inconclusive CCRTIS will screen resulting fingerprint submissions against its national repository (containing criminal and immigration fingerprints)	Not Retained.	Name Search: 3 business days Fingerprint Search – 120 Days	Name Based – CCRTIS will provide a response of either No record or Inconclusive. An Inconclusive response requires the submission of a full set of fingerprints by the client utilizing the appropriate Application Type as defined by the RCMP. CCRTIS will screen fingerprint submissions against its national fingerprint repository (containing criminal and immigration fingerprints) response details are stipulated in the current RCMP NPS-NIST Interface Control document. The exact detail of the information that is disclosed is subject to legislative requirement and business rules and varies depending on the type of submission and the results of the search. Should the information be deemed releasable, the following information is released as a paper product, either to the client, who then forwards the results to

							IRCC or to IRCC directly. **Match to Refugee or TRB**: Biographic information included in the civil submission along with IRCC unique biometric ID and RCMP ID. **Match to Criminal:** Copy of certified criminal record as maintained in the central repository by the RCMP– subject to release of information rules.
Biometric Sharing with the U.S. and FCC Partners	Anonymous TenPrint Search (ATS)	U.S. Canada Treaty on Immigration exchange. Part 19.1, s.315.22, s.315.23 IRPR	RCMP receives Fingerprints and associated number from IRCC.	CCRTIS will screen resulting fingerprint submissions against its national repository (containing criminal and immigration fingerprints).	Not Retained	3 Business Days	CCRTIS will screen fingerprint submissions against its national fingerprint repository (containing criminal and immigration fingerprints) response details are stipulated in the current RCMP NPS-NIST Interface Control document.

Service Standards and Notes:

- Normal hours of service for CCRTIS to review and respond to applicable biometric transactions will be 24 hours a day, 7 days a week, and 365 days a year. The response time is measured from receipt of the transaction by the RCMP's NIST server until when the RCMP's search result is sent to GCMS.
- Manual processing by the CCRTIS for fingerprint submissions will be carried out Monday through Friday, 7:00 to 23:00 EST.
- Service levels will be analyzed by IRCC and reported on a quarterly basis to ensure service levels are respected and revised as required.
- Any issues with these response times will be promptly escalated to senior management for resolution.
- Given RCMP's average response times for 2014 and 2015, the RCMP business objective, and IRCC's desire to have the service standards reduced to reflect actual response times, any significant increases in response times will be escalated promptly to senior management.
- IRCC may use CPIC to augment the information received as a result of submissions to CCRTIS. The use of CPIC by IRCC is subject to a separate MOU.
- The RCMP will notify IRCC a minimum of five business days prior to any planned system outages.
- IRCC will submit a purge request of an individual's immigration information within 3-5 business days of the individual becoming a citizen.

Blank Page

PROTOCOLE D'ENTENTE ENTRE LE MINISTÈRE DE LA CITOYENNETÉ ET DE L'IMMIGRATION DU CANADA (ci-après « Immigration, Réfugiés et Citoyenneté Canada » ou « IRCC ») ET LA GENDARMERIE ROYALE DU CANADA (ci-après la « GRC »). Ci-après collectivement appelés les « participants ».

ANNEXE I : Divulgation et collecte de renseignements personnels conservés dans les systèmes du Service canadien d'identification criminelle en temps réel (SCICTR) aux fins des évaluations de personnes présentant une demande d'immigration et de citoyenneté

1. CONTEXTE

Immigration, Réfugiés et Citoyenneté Canada (IRCC) est autorisé, en vertu de la *Loi sur l'immigration et la protection des réfugiés* (LIPR), la *Loi sur la citoyenneté* et les règlements d'application connexes de prendre les mesures nécessaires pour empêcher des personnes interdites de territoire en vertu des dispositions de la LIPR à entrer ou à demeurer au Canada et s'assurer que des personnes interdites de territoire n'obtiennent pas la citoyenneté.

La Gendarmerie royale du Canada (GRC) possède des renseignements personnels en vertu de la *Loi sur le casier judiciaire*, de la *Loi sur le système de justice pénale pour les adolescents* et de la LIPR. Ces renseignements sont stockés dans les systèmes du Service canadien d'identification criminelle en temps réel (SCICTR). Le SCICTR assure le maintien du dépôt national d'information sur les casiers judiciaires, qui comprend des empreintes digitales, et a le mandat de fournir un soutien opérationnel direct aux organismes d'exécution de la loi et aux communautés de la justice pénale et de la sécurité publique du Canada pour des questions criminelles, civiles et d'immigration. Ces renseignements personnels peuvent être importants pour IRCC afin de déterminer l'identité d'un demandeur et de vérifier s'il satisfait aux critères d'admissibilité relatifs à la criminalité en vertu de la LIPR et aux critères d'admissibilité prescrits par la *Loi sur la citoyenneté.*

Le SCICTR est également le fournisseur national pour les vérifications de casier judiciaire sur la base de données biométriques à des fins civiles et criminelles, et de l'environnement de vérification de sécurité pour tous les paliers de gouvernement et le grand public.

Les participants souhaitent collaborer afin d'empêcher des personnes interdites de territoire d'entrer ou de demeurer au Canada et d'empêcher des personnes interdites de territoire de se voir accorder la citoyenneté canadienne.

2. OBJET ET PORTÉE

2.1 L'objet de la présente annexe consiste à établir les rôles et les responsabilités des participants en ce qui concerne le filtrage et l'échange de renseignements personnels sur des clients d'IRCC.

2.2 Aux fins de la présente annexe, IRCC fournit des renseignements personnels à la GRC en vertu de l'alinéa 8(2)*a*) de la *Loi sur la protection des renseignements personnels*, et la GRC répond à la demande au moyen des renseignements pouvant être communiqués qui sont stockés dans les bases de données du SCICTR. Cette information sert à déterminer l'admissibilité de personnes en vertu de la LIPR, son règlement d'application et/ou la *Loi sur la citoyenneté* et à gérer l'identité. Des détails sur les renseignements qu'IRCC fournira à la GRC ainsi que sur la réponse de la GRC se trouvent à l'appendice A.

2.3 Pour la GRC, la portée des renseignements personnels couverte par la présente annexe, ainsi que sa communication, est limitée aux renseignements stockés dans les systèmes du SCICTR de la GRC.

3. DÉFINITIONS

3.1 Aux fins de la présente annexe, les termes qui sont définis dans la LIPR, le *Règlement sur l'immigration et la protection des réfugiés*, la *Loi sur citoyenneté*, le *Règlement sur la citoyenneté* ou le *Code criminel* conservent le même sens. Les termes énumérés ci-après auront le sens suivant :

a) Donnée biométrique : empreintes digitales et photographies d'un ressortissant étranger ou d'un résident permanent.

b) Représentants désignés : Principales personnes-ressources des participants chargées de surveiller la mise en œuvre de la présente annexe. Ils sont notamment responsables de l'interprétation, des demandes de renseignements et des demandes de modifications en lien avec la présente annexe. Ils doivent également régler tout problème qui en découle, y compris la conformité aux dispositions.

c) Différend : Conflit ou désaccord concernant l'un ou l'autre des points suivants :
   i. l'interprétation, l'application ou la mise en œuvre de la présente annexe; ou
   ii. la non-conformité ou la non-conformité prévue à la présente annexe.

d) Renseignements personnels : Renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, conformément à l'article 3 de la *Loi sur la protection des renseignements personnels*.

e) Atteinte à la vie privée : Collecte, utilisation, divulgation, accès, stockage ou élimination non autorisé de renseignements personnels, de façon volontaire ou accidentelle.

f) Suspension du casier judiciaire : suspension d'un casier judiciaire définie au paragraphe 2(1) de la *Loi sur le casier judiciaire*.

g) Filtrage : Détermination de l'admissibilité par IRCC au moyen de l'échange de renseignements personnels détenus par la GRC; plus précisément du Système d'identification en temps réel (SITR).

4. RESPONSABILITÉS D'IRCC

4.1 Évaluer les renseignements fournis par la GRC pour déterminer l'admissibilité en vertu de la LIPR et son règlement d'application ainsi que l'admissibilité d'individus en vertu de la *Loi sur la citoyenneté*.

4.2 Respecter les réserves relatives aux renseignements personnels pour ce qui est de leur utilisation, de leur classification ou de leur diffusion additionnelle.

4.3 Comprendre que l'exactitude des recherches d'empreintes digitales effectuées par la GRC dépend de la qualité des empreintes digitales.

4.4 Modifier et supprimer les renseignements personnels sur un individu détenus par la GRC qui sont stockés dans les dépôts de données de l'immigration au nom d'IRCC.

4.5 S'assurer que les renseignements sur l'immigration de personnes qui deviennent des citoyens canadiens sont supprimés des systèmes de la GRC dans des délais convenus par les participants.

4.6 Assumer le risque associé à la divulgation à des partenaires d'exécution de la loi des renseignements personnels sur des personnes pendant la période allant du moment où un individu devient un citoyen et la disposition des renseignements sur l'immigration, lorsque la loi le permet.

5. RESPONSABILITÉS DE LA GRC

5.1 Appuyer IRCC en effectuant des recherches dans les bases de données criminelles et de l'immigration détenues par le SCICTR et fournir à IRCC les résultats de ces recherches.

5.2 Au besoin et sur demande, fournir à IRCC des documents appropriés attestés (p. ex. dans les cas d'interdiction de territoire).

5.3 Pour donner suite à une demande de filtrage d'IRCC fondée sur le nom, déployer tous les efforts raisonnables pour fournir des renseignements sur le casier judiciaire pouvant être divulgués par la GRC sur des sujets connus d'IRCC à IRCC, et ce, dans un délai acceptable convenu par les participants.

5.4 Pour donner suite à une demande de filtrage d'IRCC fondée sur des données biométriques, déployer tous les efforts raisonnables pour fournir des renseignements sur le casier judiciaire et sur l'immigration pouvant être divulgués par la GRC sur des sujets connus d'IRCC à IRCC, et ce, dans un délai acceptable convenu par les participants.

5.5 Respecter les réserves et les limites associées aux renseignements personnels pour ce qui

est de leur utilisation, de leur classification, de leur manipulation et/ou de leur diffusion additionnelle. S'il s'agit de renseignements provenant d'un partenaire de la Conférence des cinq pays ou d'un autre partenaire international, les réserves et les limites imposées par ce partenaire s'appliqueront également.

5.6 Aviser IRCC de la suspension du casier judiciaire si des renseignements criminels sur un Canadien ont été divulgués à IRCC et que la GRC se rend compte, par la suite, qu'une suspension de casier judiciaire a été accordée en ce qui a trait aux accusations portées contre un individu.

5.7 Envoyer un message d'erreur du système à IRCC lorsque des empreintes digitales ne satisfont pas aux critères de qualité minimaux du Système automatisé d'identification dactyloscopique (SAID) [c.-à-d. soumission refusée]. La GRC effectuera un contrôle de la qualité en examinant manuellement un pourcentage convenu d'empreintes digitales refusées par le SCICTR et informera IRCC des raisons pour lesquelles les transactions n'ont pas pu être traitées.

5.8

6. RESPONSABILITÉS CONJOINTES DES PARTICIPANTS

6.1 Au besoin, les participants se consulteront avant d'apporter tout changement découlant d'une modification des politiques ou des lois du gouvernement du Canada ou d'un engagement pouvant avoir une incidence sur le nombre de transactions, des programmes spéciaux ou d'autres éléments de la présente annexe. Les participants reconnaissent que la disponibilité de fonds suffisants sera prise en considération avant toute modification du nombre de transactions ou la mise en œuvre d'un nouveau programme.

6.2 Les participants détermineront, en collaboration et conformément à la LIPR et à la *Loi sur la citoyenneté*, les renseignements personnels nécessaires pour qu'IRCC puisse déterminer l'admissibilité d'individus. Un document distinct appelé Matrice du filtrage a été élaboré afin de décrire chaque processus, les éléments de renseignements personnels connexes qu'IRCC fournit à la GRC et les résultats du filtrage des données qui sont fournis par la GRC (voir l'appendice A). La matrice sera mise à jour au besoin et examinée au même moment que l'annexe.

6.3 Les participants avisent l'autre partie immédiatement de toute panne imprévue ou inattendue des systèmes qui a une incidence sur les transactions biographiques ou biométriques.

7. CONSERVATION, UTILISATION ET DISPOSITION DE L'INFORMATION

7.1 Les participants comprennent que la période de conservation et de disposition des renseignements biométriques recueillis par IRCC est déterminée par IRCC. IRCC conserve et élimine tous les résultats du filtrage provenant des systèmes du SCICTR et fournis par la GRC conformément au calendrier de conservation et de disposition qui s'applique et comme l'exigent la *Loi sur la protection des renseignements personnels*, la *Loi sur la Bibliothèque et les Archives du Canada*, la *Loi sur le casier judiciaire* et la politique gouvernementale.

7.2 Conformément à la présente annexe et sauf si la loi le permet ou l'exige, les renseignements personnels échangés et conservés entre les participants aux fins de l'exécution du filtrage décrit dans la présente annexe ne seront pas utilisés, divulgués ou conservés pour toute autre fin que celle pour laquelle ils ont été recueillis ou créés.

8. TRANSMISSION DE L'INFORMATION

8.1 L'information couverte dans la présente annexe (appendice A) sera transmise de façon sécurisée entre les participants d'une façon conforme à leur législation, à leurs politiques et à leurs directives respectives en ce qui concerne la transmission sécuritaire d'information.

8.2 Les participants doivent prendre toutes les mesures raisonnables pour réduire le risque de transmission de programmes, de données ou de virus nuisibles dans les renseignements échangés. Ils ne peuvent pas être tenus responsables des préjudices consécutifs à la transmission de programmes, données ou virus nuisibles.

9. SÉCURITÉ DE L'INFORMATION

9.1 Chaque participant détermine la classification de sécurité de l'information qu'elle communique en vertu de la présente annexe et traite toute l'information reçue en vertu de celle-ci conformément aux cotes de sécurité qu'elle porte et aux normes du gouvernement du Canada en matière de classification de sécurité.

9.2 Les participants veuillent à ce que seuls les employés tenus, par leurs fonctions, d'avoir accès à l'information fournie par chaque organisation y aient effectivement accès et à ce que ces employés aient la cote de sécurité nécessaire.

10. REPRÉSENTANTS DÉSIGNÉS

10.1 Les représentants désignés sont les principales personnes-ressources des participants chargées de surveiller la mise en œuvre de la présente annexe. Cela comprend l'interprétation, les demandes de renseignements et les demandes de modifications

concernant la présente annexe ainsi que le traitement de toutes les questions qui en découlent.

10.2 Les personnes qui suivent sont les fonctionnaires désignés pour l'application de la présente annexe :

Pour la GRC : Directeur général
Service canadien d'identification criminelle en temps réel
1200, promenade Vanier, Ottawa (Ontario)

Pour IRCC : Directeur général,
Orientation du programme d'immigration
365, avenue Laurier Ouest, Ottawa (Ontario)

Directeur général,
Direction générale de l'orientation sur les risques pour l'intégrité (DGORI)
70, rue Crémazie, Gatineau (Québec)

10.3 Les avis découlant de la présente annexe seront transmis par écrit à l'autre participant par l'intermédiaire du représentant désigné.

11. PRÉVENTION ET RÈGLEMENT DES DIFFÉRENDS

11.1 Les participants conviennent de déployer tous les efforts raisonnables pour prévenir un différend découlant de l'interprétation ou de l'administration de la présente annexe. En cas de différend, les participants s'efforcent de régler conjointement la question à l'échelon administratif le plus bas possible.

11.2 Si un différend ne peut pas être réglé à l'amiable, les participants acheminent la question à l'échelon supérieur conformément aux procédures de règlement des différends établies dans le PE.

12. SURVEILLANCE

12.1 Les participants examineront les pratiques et les procédures établies dans la présente annexe pour s'assurer qu'elles sont conformes et que les dispositions du PE sont à jour à la date du cinquième anniversaire de sa signature, puis tous les cinq ans par la suite.

12.2 En vue de refléter tout changement découlant du projet d'élargissement de la biométrie, les participants examineront la présente annexe entre mai et novembre 2017.

12.3 Chaque participant avisera l'autre participant en cas de non-respect des modalités de la présente annexe.

13. RÉSILIATION

13.1 La présente annexe peut être résiliée de l'une des façons suivantes :

a) à tout moment si les participants en conviennent par écrit;
b) par la signature d'un participant qui signifie à l'autre un avis écrit d'au moins trois (3) mois; ou
c) par l'un ou l'autre des participants en tout temps si l'un des participants omet de respecter les obligations qui lui incombent en vertu de la présente annexe ou du PE, et après avoir suivi le processus de prévention et de règlement des différends établi à l'article 11 de l'annexe.

13.2 Les participants conviennent qu'ils doivent continuer de protéger et de préserver l'intégrité des renseignements échangés en vertu de la présente annexe, y compris de conserver et d'éliminer ces renseignements, même après la résiliation de la présente annexe.

14. MODIFICATIONS

14.1 La présente annexe peut être modifiée en tout temps avec le consentement écrit des deux participants.

15. ENTENTE COMPLÈTE

15.1 La présente annexe renferme l'entente complète entre les participants en ce qui concerne la fonction de filtrage fournie par le SCICTR de la GRC et remplace l'annexe sur le filtrage signée par les participants en 2012 et l'accord de niveau opérationnel sur la biométrie signé en 2015.

16. DISPOSITIONS FINANCIÈRES

16.1 Les participants assument leurs propres coûts lorsqu'ils échangent des renseignements aux termes de la présente annexe. Les participants assument tous les coûts supplémentaires rattachés à l'administration de la présente entente.

16.2 Les participants assument leurs propres coûts liés à l'exécution de leurs activités et obligations aux termes de la présente annexe.

17. DATE D'ENTRÉE EN VIGUEUR

17.1 La présente annexe entrera en vigueur à la date de sa signature par le dernier des signataires et le demeurera jusqu'à ce qu'on y mette un terme conformément à la

procédure établie dans la présente annexe.

18. SIGNATURES

EN FOI DE QUOI, la présente annexe a été signée en deux exemplaires, chaque exemplaire étant également valide.

Pour Immigration, Réfugiés et Citoyenneté Canada :

July 13/17

Directeur général — Date
Orientation du programme d'immigration
365, avenue Laurier Ouest, Ottawa (Ontario)

July 14/17

Directeur général — Date
Direction générale de l'orientation sur les risques pour l'intégrité (DGORI)
70, rue Crémazie, Gatineau (Québec)

Pour la Gendarmerie royale du Canada :

2017-06-15

Directeur général — Date
Service canadien d'identification criminelle en temps réel, GRC

Catégorie de filtrage	Type de transaction	Responsable du filtrage	Renseignements personnels	Processus de filtrage de la GRC	Conservation et disposition	Accord de niveau de service	Résultats du filtrage de la GRC
Filtrage biométrique de demandeurs de résidence temporaire de 29 pays et d'un territoire, conformément au *Règlement sur l'immigration et la protection des réfugiés* Filtrage biométrique des demandeurs de résidence temporaire [paragraphe 16(2) de la LIPR]	IMM	Article 36 de la LIPR R 12.1	**Biométrique :** Empreintes digitales et données biographiques connexes, conformément au document de contrôle des interfaces NIST-SNP de la GRC en vigueur	Le SCICTR effectuera la vérification des soumissions d'empreintes digitales dans son répertoire national (qui contient les empreintes digitales criminelles et de l'immigration).	Conservé dans la base de données de l'immigration de la GRC pendant 15 ans à compter de la date de la collecte des données biométriques, sauf en cas de modification ou d'obtention de la citoyenneté.	Trois jours ouvrables	Les résultats du filtrage biométrique comprennent un numéro de dossier qui correspond à un dossier d'immigration nouveau ou existant. S'il y a lieu, un numéro de dossier de réfugié existant ou un numéro FPS de casier judiciaire sera fourni. IRCC peut obtenir des renseignements additionnels au moyen du CIPC.
Demandeurs d'asile et personnes qui présentent une demande de réinstallation depuis l'étranger	IMM	Article 36 de la LIPR Paragraphe 16(2) de la LIPR	Empreintes digitales et données biographiques connexes, conformément au document de contrôle des interfaces NIST-SNP de la GRC en vigueur	Le SCICTR effectuera la vérification des soumissions d'empreintes digitales dans son répertoire national (qui contient les empreintes digitales criminelles et de l'immigration).	Conservé dans la base de données de l'immigration de la GRC jusqu'à ce que le client atteigne l'âge de 100 ans ou obtient la citoyenneté.	Trois jours ouvrables	Le SCICTR effectuera la vérification des soumissions d'empreintes digitales dans son répertoire national d'empreintes digitales (qui contient les empreintes digitales criminelles et de l'immigration). Les détails de la réponse sont décrits dans le document de contrôle des interfaces NIST-SNP de la GRC.

Filtrage biographique des demandeurs de résidence permanente – au Canada	Recherche par nom (NBS) /MAP	Article 36	**Biographique :** Nom, date de naissance (Si le nom/la date de naissance du client figure dans la base de données, ce client se voit demander de soumettre ses empreintes digitales.) **Biométrique :** Empreintes digitales et données biographiques connexes, conformément au document de contrôle des interfaces NIST-SNP de la GRC en vigueur **(soumission civile)**	**Systématique :** Vérification biographique dans le CIPC/FJN **Case par cas :** Les empreintes digitales sont requises lorsque la correspondance du nom est non concluante Le SCICTR effectuera la vérification des soumissions d'empreintes digitales dans son répertoire national (qui contient les empreintes digitales criminelles et de l'immigration).	Non conservé	Recherche par nom : Trois jours ouvrables Recherche par empreintes digitales – 120 jours	Recherche par nom – La réponse du SCICTR sera Aucun dossier ou Non concluant. Une réponse non concluante exige la soumission d'un ensemble complet d'empreintes digitales par le client au moyen du type de demande approprié défini par la GRC. Le SCICTR effectuera la vérification des soumissions d'empreintes digitales dans son répertoire national d'empreintes digitales (qui contient les empreintes digitales criminelles et de l'immigration). Les détails de la réponse sont décrits dans le document de contrôle des interfaces NIST-SNP de la GRC. Les détails exacts de l'information divulguée sont assujettis à des exigences législatives et à des règles opérationnelles et varient selon le type de soumission et les résultats de la recherche. Si on détermine que l'information peut être divulguée, les renseignements suivants sont diffusés sur papier au client, qui les transmet à

							IRCC, ou directement à IRCC. **Correspondance – réfugié ou biométrie pour les résidents temporaires :** Renseignements biographiques contenus dans la soumission civile et ID biométrique unique d'IRCC et ID de la GRC. **Correspondance – casier judiciaire:** Exemplaire attesté du casier judiciaire provenant du répertoire central de la GRC (peut être assujetti à des règles de divulgation).
Demandeur de citoyenneté	Recherche de nom /MAP	Article 36 de la LIPR Articles 21 et 22 de la *Loi sur la citoyenneté*	**Biographique** Nom, date de naissance Si le nom du client figure dans la base de données, ce client se voit demander de soumettre ses empreintes digitales directement à la GRC.	**Systématique :** Vérification biographique dans le CIPC/FJN **Cas par cas :** Les empreintes digitales sont requises lorsque la correspondance du nom est non concluante	Non conservé	Recherche par nom : Trois jours ouvrables Recherche par empreintes digitales – 120 jours	Recherche par nom – La réponse du SCICTR sera Aucun dossier ou Non concluant. Une réponse non concluante exige la soumission d'un ensemble complet d'empreintes digitales par le client au moyen du type de demande approprié défini par la GRC. Le SCICTR effectuera la vérification des soumissions d'empreintes digitales dans son répertoire national d'empreintes digitales (qui contient

				Le SCICTR effectuera la vérification des soumissions d'empreintes digitales dans son répertoire national (qui contient les empreintes digitales criminelles et de l'immigration).			les empreintes digitales criminelles et de l'immigration). Les détails de la réponse sont décrits dans le document de contrôle des interfaces NIST-SNP de la GRC. Les détails exacts de l'information divulguée sont assujettis à des exigences législatives et à des règles opérationnelles et varient selon le type de soumission et les résultats de la recherche. Si on détermine que l'information peut être divulguée, les renseignements suivants sont diffusés sur papier au client, qui les transmet à IRCC, ou directement à IRCC. **Correspondance – réfugié ou biométrie pour les résidents temporaires :** Renseignements biographiques contenus dans la soumission civile et ID biométrique unique d'IRCC et ID de la GRC. **Correspondance – casier judiciaire :** Exemplaire attesté du casier judiciaire provenant du répertoire central de la GRC (peut être assujetti à des règles de divulgation).

Échange de données biométriques avec les États-Unis et des partenaires de la Conférence des cinq pays	Recherche d'empreintes décadactylaires anonyme (ATS)	Traité Canada – États-Unis sur l'échange de renseignements en matière d'immigration Partie 19.1, articles 315.22 et s.315.23 du	La GRC reçoit les empreintes digitales et le numéro associé d'IRCC.	Le SCICTR effectuera la vérification des soumissions d'empreintes digitales dans son répertoire national (qui contient les empreintes digitales criminelles et de l'immigration).	Non conservé	Trois jours ouvrables	Le SCICTR effectuera la vérification des soumissions d'empreintes digitales dans son répertoire national d'empreintes digitales (qui contient les empreintes digitales criminelles et de l'immigration). Les détails de la réponse sont décrits dans le document de contrôle des interfaces NIST-SNP de la GRC.

Normes de service et remarques :

- Les heures de service normales du SCICTR en ce qui concerne l'examen et le traitement de transactions biométriques applicables seront de 24 heures par jour, 7 jours par semaine et 365 jours par année. Le temps de réponse est mesuré de la réception de la transaction par le serveur NIST de la GRC jusqu'à l'envoi des résultats de la recherche de la GRC au SMGC.
- Le traitement manuel par le SCICTR pour les soumissions d'empreintes digitales sera effectué du lundi au vendredi, de 7 h à 23 h (heure normale de l'Est).
- Les niveaux de service seront analysés par IRCC et signalés de façon trimestrielle pour veiller à ce que les niveaux de service soient respectés et modifiés, au besoin.
- Tout problème lié au temps de réponse sera acheminé à la haute direction immédiatement aux fins de règlement.
- Compte tenu des temps de réponse moyens de la GRC en 2014 et en 2015, l'objectif opérationnel de la GRC et le souhait d'IRCC de faire réduire les normes de service en vue de refléter les temps de réponse réels, toute augmentation considérable du temps de réponse sera acheminée à la haute direction immédiatement.
- IRCC peut utiliser le Centre d'information de la police canadienne (CIPC) pour compléter les renseignements reçus au moyen d'une soumission au SCICTR. L'utilisation du CIPC par IRCC est assujettie à un PE distinct.
- La GRC avisera IRCC au moins cinq jours ouvrables avant toute interruption prévue des systèmes.
- IRCC présentera une demande de suppression des renseignements de l'immigration d'une personne de trois à cinq jours ouvrables après que cette personne soit devenue un citoyen.

MEMORANDUM OF UNDERSTANDING BETWEEN THE DEPARTMENT OF CITIZENSHIP AND IMMIGRATION (herein referred to as "Immigration, Refugees and Citizenship Canada" or IRCC) AND THE ROYAL CANADIAN MOUNTED POLICE (herein referred to as "RCMP"). Collectively referred as the Participants

ANNEX IV: Corporate Matters

1. PURPOSE

1.1 This Annex outlines how IRCC and the RCMP will collaborate on internal and external communications and ensuring an RCMP presence in citizenship ceremonies.

2. COMMUNICATIONS

2.1 The Participants recognize that:

a) Communications will be understood to apply to internal and external communications whether carried out through community relations, public opinion research, media relations, news releases, publications, announcements and other materials, advertising, events, and postings to corporate web sites or social media.

b) Timely and coordinated communications with various external and internal audiences is desirable, especially in view of the shared mandate and common interests and needs of the Participants in the enforcement of immigration and citizenship legislation.

c) Timely and coordinated communication between the Participants is necessary through regular meetings and on-going dialogue to support mutual understanding of priorities and to plan and discharge the joint communications activities described in this MOU and its Annexes.

d) There is a need for ongoing collaboration on issue-specific initiatives, given that IRCC and RCMP individual and joint policies, programs and activities often revolve around matters of sensitivity that can involve or have an impact on other partners.

e) There is a benefit to be derived from sharing knowledge and research on migration and diversity. Consequently IRCC and the RCMP will collaborate in supporting research and promoting policy research exchanges. The aim is to improve both organizations' understanding of critical public policy issues and to strengthen their capacity to take strategic action.

f) Each participant has its own communications policies, standards, approaches, internal structures and resources to respect in managing communications as well as external requirements such as Privacy and Access to Information legislation or standards and procedures of other bodies such as Treasury Board policies on communications and federal identity.

3. COORDINATION

3.1 The Participants acknowledge that:

a) The primary coordination role will be discharged by the Directors General of Communications responsible for communications in each organization.

b) Communications coordination has as its objectives to:

- enhance strategic communications planning to maximize the communications opportunities, so as to support the operational objectives, enhance the collaborative and coordinated work of the Participants, develop integrated Government of Canada messaging as needed and ensure consistency and accuracy in messaging between the Participants;

- provide advance notification of communications activities to allow appropriate time for the Participants to be notified of events in advance so as they can prepare responsive messages. Generally, the Participants will be given time to mutually accept the over-arching and issue-specific communications goals, messages, strategies, tactics/tools and responsibilities; resolve concerns either Participant might have in advance so as to enhance and educate each other on issues and communications opportunities that are not directly linked to either organization; and,

- provide consistent interdepartmental co-ordination.

c) It is necessary to share, in a timely manner, communications initiatives, such as news releases or media lines/calls that impact or reference either or both Participants. These include major events of direct relevance to joint operations or horizontal communications management. For the purposes of this Annex, a major event is defined as an incident, event, announcement and/or speaking engagement likely to garner Canadian and/or international media attention.

d) Joint communication with their respective employees on the objectives and modalities of this MOU and of any developments to it is required.

4. PROCESS

4.1 Further to Annex II, Section 2.3, the Participants will establish a process to jointly manage, communicate and share a 'heads-up"on emerging issues that may have an urgent communications dimension and/or an immediate need to communicate with stakeholders or the Canadian public. The Participants will undertake to implement the process within sixty (60) days of this Annex coming into force.

4.2 The participants undertook to establish a process, which can be found in the Communications Arrangement (Appendix A).

5. PRATICAL MATTERS

5.1 Within the IRCC structure, communications activities can be accepted at the national or regional level. As the regional office provides the communications support to the respective local IRCC offices, RCMP detachments should expect local communications initiatives that impact IRCC's mandate to be approved by the IRCC regional office with an information 'heads-up" to the IRCC national (NHQ) office.

5.2 Within the RCMP structure, RCMP regional operations and divisions should also inform the RCMP's National Communications Services (NHQ) of any initiatives in accordance with the RCMP's Issues Management Standard Operating Procedure. Local communications initiatives related to immigration, citizenship and passport enforcement are to be cleared at a minimum by the appropriate RCMP Division communications office.

5.3 Such matters having the potential for national or international attention will be approved in consultation with the RCMP's National Communications Services Headquarters in Ottawa, in accordance with the RCMP'sMedia Relations Standard Operating Procedure.

6. PRESENCE of the RCMP AT CITIZENSHIP CEREMONIES

6.1 The citizenship ceremony is an important event wherein the government and people of Canada mark an important milestone in the lives of new citizens. The ceremony should be decorous, meaningful, and symbolic of Canada as well as fulfilling a significant community relations goal. Therefore, as an internationally recognized symbol of Canada, the RCMP member(s) attending the ceremony should be dressed in Review Order (Red Serge) which will complement favorably a citizenship ceremony.

6.2 The Participants mutually accept that:

a) The RCMP remains committed to supporting its presence at citizenship ceremonies

within its availability and on an entirely voluntary basis. As much as possible, and as resources permit, the RCMP will use its discretion to designate members attendance.

b) The RCMP will, subject to discussions at the regional and local levels, and subject to availability give priority to the following key citizenship ceremonies:

   a) Canada Day – July 1
   b) Citizenship Week – October (2nd week)
   c) Citizenship ceremonies that are identified as being particularly high profile or of significant community interest

c) The RCMP will cover in principle all costs related to RCMP ceremonial participation.

d) Requests for participation at citizenship ceremonies can be routed to the local RCMP detachment as per usual, ideally 2 weeks or more in advance.

e) Each request will be reviewed for approval and resources will be assigned based on availability and operational needs. The RCMP will endeavor to accommodate short notice, ad-hoc requests for attendance where possible.

f) The RCMP may designate either serving or retired members to attend ceremonies. Should a retired member wish to participate in a citizenship ceremony, IRCC will communicate with the local RCMP detachment to ensure that the members are aware of the activity.

g) The RCMP acknowledges that IRCC can share the name of the RCMP officer that presided at the ceremony as required (for acknowledgement before, during or after the ceremony and materials distributed at the ceremony).

h) When attending citizenship ceremonies, RCMP members will perform such ceremonial duties in Review Order (Red Serge).

i) The Participants will maintain open lines of communication and to meet as necessary to resolve any operational issues that may arise.

7. DESIGNATED REPRESENTATIVES:

7.1 Designated Representatives are the primary contacts for the Participants responsible for monitoring the implementation of this Annex. This includes the interpretation, inquiries, requests for amendments of this Annex and addressing any issues that arise from it.

7.2 For the purposes of this Annex, the following officials are the Designated Representatives:

For the RCMP: Director General
National Communication Services
73 Leikin Drive, Ottawa, Ontario

For IRCC: Director General
Communications Branch
365 Laurier Avenue West, Ottawa, Ontario

Director General,
Citizenship, Passport Program Guidance Branch
300 Slater Street, Ottawa, Ontario

7.3 Notices under this Annex will be in writing and delivered to the other Participant via the Designated Representative.

8. DISPUTE PREVENTION AND RESOLUTION

8.1 The Participants will make every reasonable effort to prevent a dispute arising from the interpretation or operation of this Annex. In the event of a dispute, the Participants will endeavor to jointly resolve the matter at the lowest administrative level possible.

8.2 In the event a dispute cannot be resolved amicably, the Participants will escalate the matter in accordance with the procedures set out in the MOU for dispute resolution.

9. MONITORING

9.1 The Participants will review the practices and procedures outlined in this Annex to ensure that the provisions of the MOU are kept up-to-date, on the five (5) year anniversary of its signing and every five (5) year anniversary forthwith, or within a mutually acceptable timeframe to the Participants.

9.2 Each Participant will notify the other Participant in the event that any terms of this Annex are not respected.

10. TERMINATION

10.1 This Annex can be terminated in one of the following ways:

a) at any time by written acceptance of the Participants;

b) by either Participant's signatory by providing at least three (3) months' notice in writing; or

c) by either Participant at any time if a Participant fails to meet its obligations under this annex or MOU, and having followed the dispute prevention and resolution provisions in Section 8 of the annex.

10.2 The Participants mutually accept that their responsibilities to protect and maintain the integrity of the information shared under this annex, including retention and disposal of the information, continue after this annex is terminated.

11. AMENDMENTS

11.1 This Annex may be amended at any time by mutual consent, in writing, of the Participants.

12. FINANCIAL ARRANGEMENTS

12.1 The Participants will bear their own costs when exchanging information under this Annex. The Participants will absorb all incremental costs associated with the operation of this arrangement.

12.2 The Participants will each bear its own costs in performing their respective activities and responsibilities under this Annex.

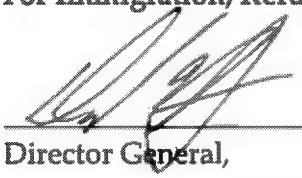
13. EFFECTIVE DATE

13.1 This Annex will become effective on the date it is signed by the last of the signatories and remain in effect until terminated in accordance with the procedures set out in this Annex.

14. SIGNATURES

IN WITNESS THEREOF, this Annex, in both official languages, was signed in duplicate, each copy being equally authentic.

For Immigration, Refugees and Citizenship Canada:



AUG 15 2017

Director General,
Communications Branch
365 Laurier Avenue West, Ottawa, Ontario

Date

Director General,
Citizenship, Passport Program
Guidance Branch
300 Slater Street, Ottawa, Ontario

Aug 2, 2017
Date

For the Royal Canadian Mounted Police:

Director General,
National Communication Services
73 Leikin Drive, Ottawa, Ontario

June 19, 2017
Date

Appendix A

Communications Arrangement

The purpose of this document is to establish an arrangement between the communications departments at the Royal Canadian Mounted Police (RCMP) and Immigration Refugees and Citizenship Canada (IRCC) for major events that impact the IRCC. A major event is defined as an incident, event, announcement and/or speaking engagement likely to garner Canadian and/or international media attention.

Objectives:

- Advance notification of communications activities
- Consistent interdepartmental co-ordination
- Enhanced strategic communications planning
- Integrated Government of Canada messaging

Notification made through this communications arrangement does not exclude the requirements for policy centers to communicate with one another through their established operational channels. This communications arrangement is meant to complement the exchange of operational communications at the policy working level. Information exchange will be reciprocal. The circulation of the information provided by RCMP Communications to IRCC Communications, or vice versa, will be treated with sensitivity and, as appropriate, will be limited to a select few senior officials at IRCC or RCMP. Information provided by RCMP Communications will not be shared by IRCC Communications (ie. Briefing to Minister) without prior approval by the RCMP. Likewise, information provided by IRCC Communications will not be shared by RCMP Communications (ie. Briefing to Minister) without prior approval by IRCC.

Specifics of the arrangement:

1. Timely communications alerts will be delivered from the media relations unit at RCMP National HQ to IRCC media relations unit at a specified to be determined email box address without delays on emerging major events. Due to sensitivities and often secret/confidential nature of information tied to these major events, it is understood that RCMP "heads ups" may vary in time. IRCC will limit membership in this email box to the Media Relations manager, lead strategist and departmental liaison. It will be the lead strategist responsibility to keep this membership list current. For Provincial/Territorial led major events the RCMP will provide a "heads up" to IRCC whenever possible. Communications products for planned, major events related to either department's

mandate are to be shared by the media relations unit at RCMP NHQ with IRCC media relations prior to public use. This includes: providing media advisories, news releases, background info, media lines and talking points for spokespersons.

2. With due regard for operational integrity, RCMP National HQ is responsible for providing IRCC with timely situational awareness with respect to public communications. Consultations with IRCC should not prevent the RCMP from engaging the public and the media in a timely manner on operational issues. The RCMP will advise IRCC, as soon as possible, on any issue that impacts them.

3. This Communications arrangement does not apply should the IRCC be the subject of an investigation by the RCMP.

Implementation:

The RCMP and IRCC will start implementing this arrangement upon signature by the designated representatives.

Monitoring and Evaluation:

The arrangement will be reviewed on a regular basis and adjusted as required. The RCMP and IRCC will meet at least annually or as needed to review procedures and make recommendations for refinements.

PROTOCOLE D'ENTENTE ENTRE LE MINISTÈRE DE LA CITOYENNETÉ ET DE L'IMMIGRATION DU CANADA (ci-après « Immigration, Réfugiés et Citoyenneté Canada » ou « IRCC ») ET LA GENDARMERIE ROYALE DU CANADA (ci-après la « GRC »). Ci-après collectivement appelés les « participants ».

ANNEXE IV : Questions ministérielles

1. OBJET

1.1 La présente annexe décrit les modalités de la collaboration d'IRCC et de la GRC en matière de communications internes et externes pour assurer la présence de la GRC aux cérémonies de citoyenneté.

2. COMMUNICATIONS

2.1 Les participants reconnaissent ce qui suit :

a) « Communications » s'appliquera à toutes les communications externes, qu'elles soient faites sous forme de relations avec les collectivités, de recherche sur l'opinion publique, de relations avec les médias, de communiqués, de publications, d'annonces et d'autres matériels, publicité, événements publics ou affichages sur les sites Web des médias sociaux et organisationnels.

b) Des communications opportunes et coordonnées avec divers publics externes et internes sont souhaitables, compte tenu surtout du mandat que se partagent les participants et de leurs intérêts et besoins communs aux fins de l'exécution de la législation en matière d'immigration et de citoyenneté.

c) Des communications opportunes et coordonnées entre les participants doivent avoir lieu au moyen de réunions périodiques et d'un dialogue constant visant à soutenir une compréhension mutuelle des priorités et à planifier et réaliser les activités de communication communes décrites dans le présent protocole d'entente (PE) et ses annexes.

d) Une collaboration constante est nécessaire à propos d'initiatives portant sur des enjeux particuliers, étant donné que les politiques, les programmes et les activités d'IRCC et de la GRC, qu'ils soient propres à chaque partie ou communs, portent souvent sur des renseignements sensibles qui peuvent viser d'autres partenaires ou avoir une incidence sur eux.

e) L'échange de connaissances et de résultats de recherche sur la migration et la diversité peut comporter des avantages. Par conséquent, IRCC et la GRC collaboreront en vue d'appuyer des recherches et de favoriser le partage des

résultats des recherches stratégiques. L'objectif est d'amener les deux organisations à mieux comprendre les enjeux déterminants des politiques publiques et de renforcer leur capacité à prendre des mesures stratégiques.

f) Chaque participant doit se conformer à ses propres politiques, normes, approches, structures internes et ressources en matière de gestion des communications, ainsi qu'à des obligations externes, y compris la *Loi sur la protection des renseignements personnels* et la *Loi sur l'Accès à l'information*, ou aux normes et procédures d'autres organismes, notamment aux politiques du Conseil du Trésor sur les communications et à la coordination de l'image de marque au sein du gouvernement fédéral.

3. COORDINATION

3.1 Les participants reconnaissent ce qui suit :

a) La coordination principale est assurée par les directeurs généraux responsables des communications dans chaque organisation.

b) La coordination des communications vise les objectifs suivants :

- améliorer la planification des communications stratégiques en vue de maximiser les occasions de communications en vue d'appuyer les objectifs opérationnels, d'améliorer les travaux collaboratifs et coordonnés des participants, de rédiger des messages intégrés du gouvernement du Canada, au besoin, et de veiller à l'uniformité et à l'exactitude des messages échangés par les participants;

- signaler les activités de communication au préalable afin de donner aux participants le temps requis pour prendre connaissance des événements à venir et de préparer des messages complémentaires. Habituellement, les participants auront le temps d'accepter mutuellement les objectifs, messages, stratégiques, tactiques/outils et responsabilités généraux et portant sur des enjeux précis en matière de communication; d'aborder à l'avance les préoccupations de l'un ou l'autre des participants pour que les participants puissent s'améliorer et se renseigner sur des questions et des occasions de communication qui ne sont pas directement liées à l'une ou l'autre des organisations; et

- fournir une coordination interministérielle uniforme.

c) Chaque partie se doit de communiquer en temps opportun à l'autre partie les initiatives en matière de communications, comme des communiqués et/ou des

infocapsules, qui ont une incidence ou portent sur un des participants ou les deux. Cela comprend les événements majeurs qui sont directement importants pour les opérations conjointes ou la gestion horizontale des communications. Aux fins de la présente annexe, un événement majeur constitue un incident, un événement, une annonce et/ou une allocution susceptibles de susciter l'attention des médias canadiens ou internationaux.

d) La communication conjointe avec les employés de chaque participant sur les objectifs et les modalités du présent PE et de toute modification de celui-ci est requise.

4. PROCESSUS

4.1 Pour donner suite à la section 2.3 de l'annexe II, les participants établiront un processus visant à gérer, à communiquer et à échanger conjointement des avis sur des nouvelles questions pouvant constituer une urgence en matière de communication et/ou un besoin urgent de communiquer avec des intervenants ou avec le public canadien. Les participants tenteront de mettre en œuvre ce processus dans les 60 jours qui suivent l'entrée en vigueur de la présente annexe.

4.2 Les participants ont convenus d'établir un processus, et ce dernier se trouve dans les arrangements en matière de communications (appendice A).

5. QUESTIONS PRATIQUES

5.1 Au sein de la structure d'IRCC, les activités de communication peuvent être approuvées au niveau national ou régional. Comme le bureau régional fournit un soutien en matière de communications aux bureaux locaux d'IRCC respectifs, les détachements de la GRC devraient s'attendre à ce que toute initiative de communications locale ayant une incidence sur le mandat d'IRCC soit approuvée par le bureau local d'IRCC et qu'un avis soit envoyé au bureau national d'IRCC (Administration centrale [AC]).

5.2 Au sein de la structure de la GRC, les opérations régionales et les divisions doivent également informer les Services de communication nationaux (Direction générale [DG]) de ces initiatives, conformément à la procédure normalisée d'exploitation de la GRC concernant la gestion des questions d'intérêt. Les initiatives de communication locales liées à l'exécution de la législation en matière d'immigration, de citoyenneté et de passeports sont autorisées à tout le moins par le bureau des communications de la division appropriée de la GRC.

5.3 Les communications susceptibles d'attirer l'attention à l'échelle nationale ou internationale sont approuvées après la consultation des Services de communication

nationaux de la GRC, à la Direction générale à Ottawa, conformément à la procédure normalisée d'exploitation de la GRC concernant les relations avec les médias.

6. PRÉSENCE de la GRC AUX CÉRÉMONIES DE CITOYENNETÉ

6.1 La cérémonie de citoyenneté est un événement important au cours duquel le gouvernement et la population du Canada soulignent une étape marquante dans la vie des nouveaux citoyens. La cérémonie doit être respectueuse, marquante et représentative du Canada, et atteindre un objectif important au chapitre des relations communautaires. Cela dit, comme l'uniforme de la GRC constitue un symbole du Canada reconnu à l'étranger, le ou les membres de la GRC qui participent à une cérémonie doivent porter leur tenue de parade (tunique rouge). Cette tenue sera bien accueillie lors d'une cérémonie de citoyenneté.

6.2 Les participants acceptent mutuellement ce qui suit :

a) La GRC demeure engagée à appuyer sa présence aux cérémonies de citoyenneté selon ses disponibilités et d'une façon entièrement bénévole. Dans la mesure du possible, et lorsque les ressources le permettent, la GRC décidera de désigner des membres aux fins de leur participation à une cérémonie.

b) La GRC, après en avoir discuté à l'échelle régionale et locale et selon la disponibilité de ses membres, accordera la priorité aux cérémonies de citoyenneté clés suivantes :

   a) Fête du Canada – 1er juillet
   b) Semaine de la citoyenneté – octobre (2e semaine)
   c) Cérémonies de citoyenneté à grande visibilité ou ayant un intérêt communautaire considérable

c) En principe, la GRC assumera tous les coûts liés à la participation de ses membres à des cérémonies.

d) Les demandes de participation à des cérémonies de citoyenneté peuvent être acheminées au détachement de la GRC local, comme d'habitude (idéalement deux semaines à l'avance).

e) Chaque demande sera évaluée, et les ressources seront affectées en fonction de la disponibilité des membres et des besoins opérationnels. La GRC participera aux cérémonies à court préavis ou spéciales, si possible.

f) La GRC peut désigner des membres de service ou retraités aux fins de la participation à des cérémonies. Si un membre retraité souhaite participer à une cérémonie de citoyenneté, IRCC communiquera avec le détachement de la GRC

local pour veiller à ce que les membres soient au courant de l'activité.

g) La GRC reconnaît qu'IRCC peut diffuser le nom de l'agent de la GRC qui a présidé à la cérémonie, s'il y a lieu (à des fins de reconnaissance avant, pendant ou après la cérémonie et dans le matériel distribué à la cérémonie).

h) Lorsqu'ils assistent à une cérémonie de citoyenneté, les membres de la GRC exécuteront leurs tâches cérémoniales en tenue de parade (tunique rouge).

i) Les participants entretiennent des communications ouvertes et se réunissent au besoin pour régler tout problème pouvant survenir.

7. REPRÉSENTANTS DÉSIGNÉS

7.1 Les représentants désignés sont les principales personnes-ressources des participants chargées de surveiller la mise en œuvre de la présente annexe. Cela comprend l'interprétation, les demandes de renseignements et les demandes de modifications concernant la présente annexe ainsi que le traitement de toutes les questions qui en découlent.

7.2 Les personnes qui suivent sont les fonctionnaires désignés pour l'application de la présente annexe :

Pour la GRC : Directeur général
Services nationaux de communication
73, promenade Leikin, Ottawa (Ontario)

Pour IRCC : Directeur général
Direction générale des communications
365, avenue Laurier Ouest, Ottawa (Ontario)

Directeur général
Direction générale de l'orientation des programmes
de citoyenneté et de passeport
300, rue Slater, Ottawa (Ontario)

7.3 Les avis découlant de la présente annexe seront transmis par écrit à l'autre participant par l'intermédiaire du représentant désigné.

8. PRÉVENTION ET RÈGLEMENT DES DIFFÉRENDS

8.1 Les participants conviennent de déployer tous les efforts raisonnables pour prévenir un différend découlant de l'interprétation ou de l'administration de la présente annexe. En

cas de différend, les participants s'efforcent de régler conjointement la question à l'échelon administratif le plus bas possible.

8.2 Si un différend ne peut pas être réglé à l'amiable, les participants acheminent la question à l'échelon supérieur conformément aux procédures de règlement des différends établies dans le PE.

9. SURVEILLANCE

9.1 Les participants doivent examiner les pratiques et les procédures établies dans la présente annexe pour s'assurer qu'elles sont conformes et que les dispositions du PE sont à jour à la date du cinquième anniversaire de sa signature, puis tous les cinq ans par la suite, ou conformément aux délais convenus par les participants.

9.2 Chaque participant avisera l'autre participant en cas de non-respect des modalités de la présente annexe.

10. RÉSILIATION

10.1 La présente annexe peut être résiliée de l'une des façons suivantes :

a) à tout moment si les participants en conviennent par écrit;

b) par la signature d'un participant qui signifie à l'autre un avis écrit d'au moins trois (3) mois; ou

c) par l'un ou l'autre des participants en tout temps si l'un des participants omet de respecter les obligations qui lui incombent en vertu de la présente annexe ou du PE, et après avoir suivi le processus de prévention et de règlement des différends établi à l'article 8 de l'annexe.

10.2 Les participants conviennent qu'ils doivent continuer de protéger et de préserver l'intégrité des renseignements échangés en vertu de la présente annexe, y compris de conserver et d'éliminer ces renseignements, même après la résiliation de la présente annexe.

11. MODIFICATIONS

11.1 La présente annexe peut être modifiée en tout temps avec le consentement écrit des deux participants.

12. DISPOSITIONS FINANCIÈRES

12.1 Les participants assument leurs propres coûts lorsqu'ils échangent des renseignements aux termes de la présente annexe. Les participants assument tous les coûts supplémentaires rattachés à l'administration de la présente entente.

12.2 Les participants assument leurs propres coûts liés à l'exécution de leurs activités et obligations aux termes de la présente annexe.

13. DATE D'ENTRÉE EN VIGUEUR

13.1 La présente annexe entrera en vigueur à la date de sa signature par le dernier des signataires et le demeurera jusqu'à ce qu'on y mette un terme conformément à la procédure établie dans la présente annexe.

14. SIGNATURES

EN FOI DE QUOI, la présente annexe, rédigée dans les deux langues officielles, a été signée en deux exemplaires, chaque exemplaire étant également valide.

Pour Immigration, Réfugiés et Citoyenneté Canada :

AUG 15 2017

Directeur général, Date
Direction générale des communications
365, avenue Laurier Ouest, Ottawa (Ontario)

02 août 2017

Directeur général, Date
Direction générale de l'orientation des programmes de citoyenneté et de passeport
300, rue Slater, Ottawa (Ontario)

Pour la Gendarmerie royale du Canada :

19 juin 2017

Directeur général Date
Services nationaux de communication
73, promenade Leikin, Ottawa (Ontario)

Appendice A

Entente en matière de communications

L'objet du présent document consiste à conclure une entente entre les responsables des communications de la Gendarmerie royale du Canada (GRC) et d'Immigration, Réfugiés et Citoyenneté Canada (IRCC) pour les événements majeurs qui ont une incidence sur IRCC. Un événement majeur est un incident, une activité, une annonce et/ou une allocution susceptibles de susciter l'attention des médias canadiens et/ou internationaux.

Objectifs :

- Une notification préalable des activités de communications
- Une coordination interministérielle uniforme
- Une planification stratégique améliorée des communications
- Des messages intégrés du gouvernement du Canada

La notification effectuée dans le cadre de la présente entente en matière de communications n'exclut pas l'obligation pour les centres de décision de communiquer entre eux au moyen des mécanismes opérationnels établis. La présente entente en matière de communications vise à compléter l'échange de communications opérationnelles au niveau des travaux stratégiques. L'échange de renseignements sera réciproque. La circulation de l'information fournie par les Communications de la GRC aux Communications d'IRCC, ou vice-versa, sera traitée d'une façon appropriée et, au besoin, ne sera divulguée qu'à quelques cadres supérieurs sélectionnés à IRCC ou à la GRC. L'information fournie par les Communications de la GRC ne sera pas diffusée par les Communications d'IRCC (c.-à-d. présentation à l'intention du ministre) sans l'obtention de l'approbation préalable de la GRC. De même, l'information fournie par les Communications d'IRCC ne sera pas diffusée par les Communications de la GRC (c.-à-d. présentation à l'intention du ministre) sans l'obtention de l'approbation préalable d'IRCC.

Éléments précis de l'entente :

1. En cas d'événement majeur, le groupe des relations avec les médias de la Direction générale (DG) de la GRC fournira immédiatement des alertes au groupe des relations avec les médias d'IRCC à une adresse électronique spécifique. En raison de la nature délicate et souvent secrète ou confidentielle de l'information liée à ces événements majeurs, il se peut que le temps requis pour communiquer les avis de la GRC varie. IRCC ne permettra qu'au gestionnaire des relations avec les médias, au stratège en chef et à l'agent de liaison ministériel d'accéder à cette boîte de messagerie. Il incombera au

stratège en chef de tenir à jour la liste des personnes ayant accès à la boîte de messagerie. Pour les événements majeurs dirigés par une province ou un territoire, la GRC fournira un avis à IRCC dans la mesure du possible. Le groupe des relations avec les médias de la DG de la GRC et le groupe des relations avec les médias d'IRCC doivent s'échanger tout produit de communications pour des événements majeurs planifiés liés au mandat de l'une ou l'autre des organisations avant de les diffuser au public. Cela comprend : fournir des avis aux médias, des communiqués, des fiches d'information, des infocapsules et des notes d'allocution pour les porte-parole.

2. Dans le respect de l'intégrité opérationnelle, les Communications de la DG de la GRC sont chargées d'informer en temps opportun les Communications d'IRCC des produits de communication publique. Les consultations auprès d'IRCC ne doivent pas empêcher la GRC de mobiliser rapidement le public et les médias sur des questions opérationnelles. La GRC avisera IRCC dès que possible de toute question ayant des répercussions sur celui-ci.

3. La présente entente en matière de communications ne s'applique pas si la GRC enquête sur IRCC.

Mise en œuvre :

La GRC et IRCC amorceront la mise en œuvre de la présente entente dès sa signature par les représentants désignés.

Surveillance et évaluation :

L'entente sera examinée régulièrement et modifiée, au besoin. La GRC et IRCC se réuniront au moins une fois par an ou selon les besoins en vue d'examiner les procédures et recommander des améliorations.

Pages 65 to / à 81

are withheld pursuant to sections

sont retenues en vertu des articles

16(1)(b), 16(1)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

IRCC-RCMP MOU Annex II – List of IRCC Designated Officials

This will be updated annually at the working level, or as deemed necessary by the Participants. This is understood to provide the RCMP with direction on whom they should contact in relation to activities as listed in the *IRCC-RCMP MOU Annex II: Investigations and Referrals for Prosecution (2021).* Information collected through parties listed in this document may not be shared with a separate party other than with CBSA as indicated below.

1. Collection and Disclosure of Information (non-8(2)(e) or (f))

1.1. For matters involving potential implications to passport entitlement (not related to national security), please contact the Centralized Network's Passport Tactical Intelligence Unit, which operates 24 hours a day, 7 days a week, 365 days a year.

- Email: @cic.gc.ca*
- Tel:
- Officials: Analysts, Program Officers, Operations Manager

* Please note that this is **not** a secured mailbox. Encrypted files may be sent directly to officials of CN's Passport Tactical Intelligence Unit.

1.2. For matters concerning national security and/or the prevention of terrorism, contact Case Management Branch's Security Cases Unit.

- Email: @cic.gc.ca*
- Officials: Analysts, Assistant Director

* Please note that this is **not** a secured mailbox. Encrypted emails are not accepted. If the information/document is sensitive the Security Cases Unit will provide the requester with a classified email address to use.

1.3. For requests related to the *Security of Canada Information Disclosure Act* (SCIDA) and for requests related to the *Secure Air Travel Act* (SATA) please contact Case Management Branch's Security Division.

- Email: @cic.gc.ca
- Officials: Analysts, Assistant Director

1.4. For all other matters without potential implications to passport entitlement or national security, contact IRCC's Access to Information and Privacy (ATIP) Section.

- Email: @cic.gc.ca
- Tel:
- Officials: ATIP Liaison Officers

s.16(2)

IRCC-RCMP MOU Annex II – List of IRCC Designated Officials

2. Confirmation of Citizenship

2.1. Contact Citizenship and Passport Cases Division's Cases and Advice Unit.

- Email: @cic.gc.ca
- Officials: Analysts

3. Document Analysis and Seizures

3.1. Contact the Domestic Network's Risk Assessment Office (foreign passports, travel and identity).

- Email: @cic.gc.ca
- Officials: Risk Assessment Officers

3.2. Contact CBSA's Document Intelligence office.

- Email: @cbsa-asfc.gc.ca.ca
- Officials: Senior Program Officers or Advisors

4. Facial Recognition System Queries

4.1. Please contact the Centralized Network's Passport Tactical Intelligence Unit, which operates 24 hours a day, 7 days a week, 365 days a year.

- Email: @cic.gc.ca
- Tel: 819-934-3159 (24/7)
- Officials: Analysts, Program Officers, Operations Manager

4.2. For national security related matters, during regular work hours, please contact Case Management Branch's Security Cases Unit at.

- Email: @cic.gc.ca
- Officials: Analysts, Assistant Director

Note that in order to do a facial recognition check for a national security investigation, we will require a SCIDA request.

5. Malfeasance (employee misconduct) Investigations

5.1. Please contact the Chief Security Officer's Corporate Security Division, Corporate Security.

- Email: @cic.gc.ca
- Officials: Personnel Security Manager; Assistant Director Administration, Security and Accommodation, Director of Corporate Security, Administration, Security and Accommodation

IRCC-RCMP MOU Annex II – List of IRCC Designated Officials

6. Passport Refusal, Revocation, and Cancellation

6.1. Please contact the Centralized Network's Passport Tactical Intelligence Unit, which operates 24 hours a day, 7 days a week, 365 days a year.

- Email: @cic.gc.ca
- Telephone:
- Officials: Analysts, Program Officers, Operations Manager

6.2. For passport-related matters that concern national security and/or the prevention of terrorism, contact Case Management Branch's Security Cases Unit.

- Email: @cic.gc.ca
- Officials: Analysts, Assistant Director

7. *Privacy Act* 8(2)(e) Requests for Information

7.1. Contact the Access to Information and Privacy (ATIP) Division.

- Email: @cic.gc.ca*
- Tel: N/A, available upon request
- Mailing Address: Access to Information and Privacy Division
  Immigration, Refugees and Citizenship Canada
  360 Laurier Avenue West
  Ottawa, Ontario, K1A 1L1
- Officials: Team Coordinators, ATIP Clerks

* Please note that this is **not** a secured mailbox. For instructions on how to provide an encrypted email, please contact the generic mailbox.

In order for IRCC to provide RCMP with information under paragraph 8(2)(e) of the *Act*, we will require a written request containing the following information:

- the name of the investigative body;
- the name of the individual who is the subject of the request, or some other personal identifier;
- the purpose of the request and a description of the information to be disclosed;
- the section of the federal or provincial statute under which the investigative activity is being undertaken;
- the hand-written signature of RCMP's Inspector, Superintendent, Chief Superintendent, Assistant Commissioner, Deputy Commissioner, Commissioner, Director General, Director, Commanding Officer, or Criminal Operations (CROPS) Officer.

IRCC-RCMP MOU Annex II – List of IRCC Designated Officials

8. Privacy Act 8(2)(m)(i) and (ii) Requests for Information

8.1. Contact IRCC's Privacy Assessment Unit, within the ATIP Section.

- Email: @cic.gc.ca*
- Telephone: "Upon request" depending on the nature of the inquiry (no generic phone number available)
- Officials: Policy Advisors

* Please note that this mailbox **does** accept encrypted emails.

9. Referrals of Revocations of Citizenship and Abuses of Citizenship Certificates

9.1. Contact Case Management Branch's Citizenship and Passport Cases Division's Revocations Unit.

- Email: @cic.gc.ca
- Officials: Analysts and Senior Analysts

10. Requests for Affidavits, Production Orders, and Court Documents

10.1. Contact Case Management Branch's Litigation Management Division, Court Coordination group.

- Email: @cic.gc.ca
- Officials: Litigation Analysts, Assistant Director

11. Seized/Surrendered/Found Canadian Passports and Other Travel Documents

11.1. Please contact the Centralized Network's Passport Tactical Intelligence Unit, which operates 24 hours a day, 7 days a week, 365 days a year.

- Email: @cic.gc.ca
- Telephone:
- Mailing Address:

- Officials: Analysts, Program Officers, Operations Manager

IRCC-RCMP MOU Annex II – List of IRCC Designated Officials

12. Visa/eTA Cancellations and Revalidations

12.1. For general visa/eTA cancellations and revalidations contact the IRCC eTA supervisors group.

- Email: @cic.gc.ca
- Officials: Forms Control Officers, Officers

Process: Forms Control Officer authorizes cancellation; Officer sets the counterfoil status to cancelled; Officer or support staff voids the affixed counterfoil in passport with a designated stamp.

12.2. For matters that concern national security and/or the prevention of terrorism, contact Case Management Branch's Security Cases Unit.

- Email: @cic.gc.ca
- Officials: Analysts, Assistant Director

13. Visa/eTA Refusals

13.1. Please contact the Irregular Migration and Risk Intelligence, International Network, Generic mailbox:

- Email: @cic.gc.ca
- Officials: Risk Assessment Officers

PRIVACY IMPACT ASSESSMENT REPORT

CIC – RCMP MOU

Citizenship and Immigration Canada

April 24, 2012

Table of Contents

Document Change Control Table

Version Number	Date of Issue	Author(s)	Brief Description of Change(s)
01	Feb15/2012	John Kent	First Draft
02	Feb29/2012	Holly McCracken/ John Kent	Second Draft
03	Feb29/2012	Sébastien Fleurant	ATIP Review
04	Mar01/2012	Jean-Francois Aube	Legal Services Review
05	Mar08/2012	John Kent	Final CIC Draft Review
06	Apr11/12	John Kent/Greg Myatt	RCMP Review

1. Executive Summary

This report is a Privacy Impact Assessment (PIA) for the renewal of the Memorandum of Understanding between Citizenship and Immigration Canada (CIC) and the Royal Canadian Mounted Police (RCMP). The partnership between CIC and the RCMP is vital to ensuring the effective administration and enforcement of the *Immigration and Refugee Protection Act* (IRPA), and the *Citizenship Act*. The key objectives of the CIC-RCMP partnership are to preserve the integrity of Canada's immigration, refugee and citizenship programs; to maintain and protect the health, safety and security of Canadians; and to promote international order and justice by denying the use of Canadian territory to persons who are likely to engage in criminal activity. The MOU includes annexes covering criminal screening, intelligence sharing, referrals for prosecutions, RCMP attendance at citizenship ceremonies, and communications.

This report analyzed all aspects of the MOU and annexes where personal information is shared. The MOU and annexes contain significant safeguards for the protection of personal information in line with new TBS requirements. The report identified three areas in the sharing of personal information: criminal screening; intelligence sharing; and referrals for prosecutions. Each area was examined in terms of privacy risk. No risks were identified in relation to intelligence sharing and referrals for prosecutions. Risk was identified in the context of criminal screening, specifically with respect to access and use of personal information. The report outlines detailed mitigation strategies in order to address these risks.

2. Introduction

2.1 Report Objectives

This Privacy Impact Assessment (PIA) has been prepared by CIC's Operational Management and Coordination Branch (OMC).

The objectives of this report are:

- To determine if there are privacy risks associated with the implementation of the new MOU and annexes
- Where risks are identified, to establish mitigation strategies to address them
- To ensure that privacy is considered throughout the project development cycle. The result of a privacy impact assessment is documented assurance that privacy issues have been identified and adequately addressed.

2.2 Scope of PIA

The following tasks outline the scope of the PIA relating to the CIC-RCMP MOU, and set out the deliverables in the form of a PIA report, in accordance with the **2002 Treasury Board Secretariat PIA guidelines** and Policy on Privacy Impact Assessments and the *Privacy Act.*

a. Description of the overall proposal summarising the project, including objectives, rationale, impact upon clients, approach, programs and or partners;
b. Data flow tables for all the data elements that involve personal information and related descriptions of the data flow and overall business diagram and a completed Privacy Analysis Questionnaire A;
c. List of relevant legislation and regulations having a bearing on privacy requirements of the proposal including any departmental program statutes and policies;
d. Identification and description of each of the areas where personal information is exchanged under the MOU
e. Description and analysis of privacy risks that have been identified through the PIA process;
f. In-depth analysis of any areas of significant risk in the exchange of personal information under this MOU
g. Possible options and/or recommendations to eliminate or mitigate privacy risks including regulatory options, with a statement of the implications associated within those mechanisms where relevant, including, if appropriate, information on similar proposals and privacy risks identified in other jurisdictions and how those risks were handled;
h. Description of any residual or outstanding risks that cannot be addressed through the mitigation mechanisms.

Out of Scope: This review does not include upcoming initiatives relating to biometric screening of temporary resident applicants (related to the Temporary Resident Biometrics Project) and screening under refugee reform pilot. Separate PIAs will be conducted for these initiatives.

2.3 Reference Documentation

CIC-RCMP Memorandum of Understanding (draft)

Annex 1: Screening (draft)

Annex 2: Referral for Prosecutions (draft)

Annex 3: Intelligence Gathering (draft)

Annex 4: Communications (draft)

PIA Specific:

Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks

Criminal Screening Matrix – Appendix A

2.4 Participants

The following participants contributed to the development of this PIA:

- John Kent, CIC OMC Branch
- Jean-Francois Aube, CIC Legal Services
- Don Mccoll, CIC ATIP
- Sébastien Fleurant, CIC ATIP
- Omid Maani, CIC Refugee Branch
- Marissa Rosenhek, CIC Refugee Branch
- Holly McCracken, CIC Admissibility Branch
- Joelle Mackenzie, CIC TR Biometrics Project
- Robert Thompson, CIC TR Biometrics Project
- Lara Armit, CIC Case Management Branch
- Peter Stockdale, CIC International and Intergovernmental Relations
- Greg Myatt, RCMP Immigration and Passport

- Pierre Nezan, RCMP, Security and Intelligence Background Section
- Benoit Belanger, RCMP, Security and Intelligence Background Section
- Dennis Goulet, RCMP, CCRTIS Policy Centre
- Brett Bush, CBSA NSSD

2.5 Legislation and Policies

The following legislation and policies were considered as part of this PIA:

Legislation:

- **Privacy Act**
  (For information, see: http://laws.justice.gc.ca/en/P-21/index.html)
- **Privacy Regulations**
  (For information, see: http://laws.justice.gc.ca/eng/SOR-83-508/index.html)
- **Personal Information and Electronic Documents Act**
  (For information, see: http://laws.justice.gc.ca/en/P-8.6/)
- **Access to Information Act**
  (For information, see: http://laws.justice.gc.ca/eng/A-1/index.html)
- **Access to Information Regulations**
  (For information, see: http://laws.justice.gc.ca/eng/SOR-83-507/index.html)
- **Immigration and Refugee Protection Act**
- **Immigration and Refugee Protection Regulations**
- **Citizenship Act**
- **Citizenship Regulations**
- **Department of Citizenship and Immigration Act**
- **Royal Canadian Mounted Police Act**
- **Royal Canadian Mounted Police Regulations**

- **Criminal Code of Canada**
- **Criminal Records Act**
- **Youth Criminal Justice Act**
- **Identification of Criminals Act**
- **Charter of Rights and Freedoms**

Policies:

- Treasury Board of Canada Secretariat *Policy on Privacy Protection* and related policy instruments (For information, see: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510)
- Treasury Board of Canada Secretariat *Policy on Access to Information* and related policy instruments (For information, see: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12453)
- CIC Privacy Impact Assessment Handbook (http://cicintranet.ci.gc.ca/connexion/info-tech/atip-aiprp/pol/pia-efvp-eng.aspx)
- CIC Information Sharing Policy (http://cicintranet.ci.gc.ca/Manuals/index_e.asp?newpage=immigration/in/index_e.asp)

Directives:

- Directive on Privacy Impact Assessment (For information, see: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308)
- Directive on Privacy Practices (For information, see: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309)
- Directive on Privacy Requests and Correction of Personal Information (For information, see: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18311)
- Directive on the Administration of the Access to Information Act (For information, see: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18310)

2.6 Abbreviations Used in this Report

The following is a list of abbreviations and acronyms used in the report:

PIA ..... Privacy Impact Assessment
TBS ……..… .. Treasury Board of Canada Secretariat
RCMP……...Royal Canadian Mounted Police
CIC……...Citizenship and Immigration Canada
IRPA……..Immigration and Refugee Protection Act
TRBP……Temporary Resident Biometric Project
R&D……...Retention and Disposition Schedule
CBSA……Canadian Border Services Agency
NSSD……..National Security Screening Division (CBSA)
ATIP…….. Access to Information and Privacy
OMC…….. Operations and Management Coordination Branch (CIC)
CPIC……...Canadian Police Information Centre (RCMP)
CNI……Criminal Name Index (RCMP)
AFIS……Automated Fingerprint Information System (RCMP)
CCRTIS……...Canadian Criminal Real Time Identification Services (RCMP)
PROS……...Police Reporting and Occurrence System (RCMP)

3. Project Proposal

Background
The partnership between Citizenship and Immigration Canada (CIC) and the Royal Canadian Mounted Police (RCMP) is vital to ensuring the effective administration and enforcement of the *Immigration and Refugee Protection Act* (IRPA), the *Citizenship Act* and other applicable Acts of Parliament. The key objectives of the CIC-RCMP partnership are to preserve the integrity of Canada's immigration, refugee and citizenship programs; to maintain and protect the health, safety and security of Canadians; and to promote international order and justice by denying the use of Canadian territory to persons who are likely to engage in criminal activity.

CIC is responsible for facilitating the arrival of people and their integration into Canada in a way that maximizes their contribution to the country while protecting the health, safety and security of Canadians. The Department also: maintains Canada's humanitarian tradition by protecting refugees and people in need of protection; promotes the rights and responsibilities of Canadian citizenship; and facilitates increased intercultural understanding to foster an integrated society with equal opportunity for all, regardless of race, ethnicity and religion. These objectives are achieved through the administration of the IRPA and the *Immigration and Refugee Protection Regulations*; the *Department of Citizenship and Immigration Act*; the *Citizenship Act* and *Regulations;* and the *Canadian Multiculturalism Act*.

The RCMP's responsibilities include, but are not limited to, combating terrorism, organized crime and specific crimes and offences that threaten the integrity of Canada's national borders. The RCMP maintains or has access to national data repositories and national databases that include fingerprints, criminal records, the Canadian Police Information Centre (CPIC) and the Automated Criminal Intelligence Information System. The RCMP's mandate is fulfilled through the administration of the *Royal Canadian Mounted Police Act*, *Royal Canadian Mounted Police Regulations*, the *Criminal Code of Canada* and its common law powers.

Proposal
The purpose of a renewed CIC-RCMP MOU is multifold: i) to ensure compliance with new Treasury Board requirements on information sharing; ii) to provide the framework for upcoming partnership programs such as biometric screening and refugee reform screening; and iii) to ensure key business processes between the two organizations remain relevant and appropriate given the new alignments of organizational responsibilities between CIC and the Canada Border Services Agency (CBSA). In general terms the renewed MOU defines the basis for cooperation and coordination between CIC and the RCMP, including the roles and responsibilities of each organization, regarding managing access to Canada and preventing inadmissible persons from remaining in Canada through:

- information sharing and information protection;
- communication;
- fingerprinting and screening, as required, of foreign nationals or permanent residents;
- developing, analysing and distributing immigration and citizenship-related intelligence;
- investigating and, when appropriate, referring for prosecution offences contrary to the IRPA and the *Citizenship Act*
- RCMP presence at citizenship ceremonies.

Although this review does not specifically include upcoming biometric screening for temporary resident applicants (the TRBP) and Refugee Reform screening initiatives, a key objective of the process is to

ensure that the new MOU framework has the established principles, accountability structures, monitoring provisions, and governance mechanisms to implement new programs as they arise. Separate PIAs will be conducted for both the TRBP and Refugee Reform initiatives.

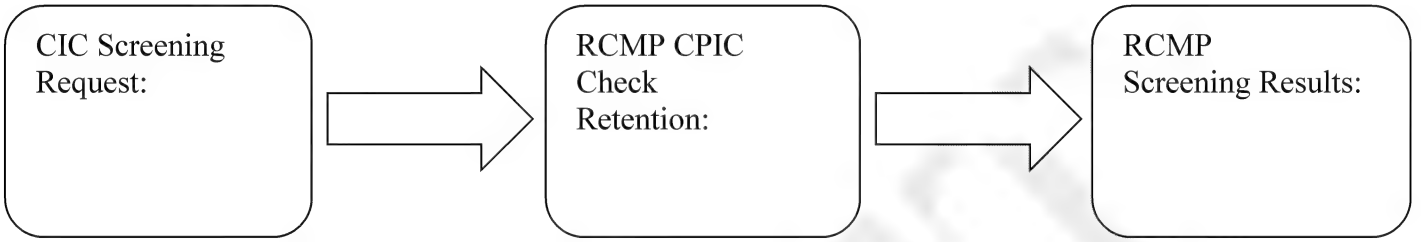
s.16(1)(b)

s.16(1)(c)

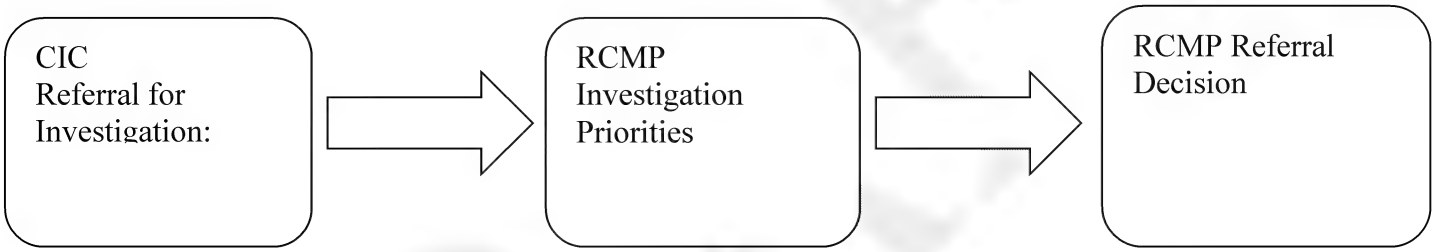
4. Data Flow Analysis

4.1 Business Flow Diagram

RCMP Screening Process:



Referral for Investigation and Prosecution:



** There may be circumstances where the RCMP will not be able to disclose results (i.e. ongoing investigation) – see section 4.7 screening annex.

4.2 Data Flow Table: Overview of Criminal Screening Process

A more complete data flow analysis outlining each aspect of RCMP screening process is attached as appendix A.

Note: Biometric screening of temporary resident applicants to be implemented in 2013 is not included in the following chart as a separate PIA will be completed as part of the Temporary Resident Biometrics Project.

Screening Category	Screening Authority	Personal Information	RCMP Screening Process	Retention and Disposition

5. Privacy Analysis

5.1 Privacy Risk Overview

The RCMP MOU covers three areas involving the potential exchange of personal information:

1. RCMP Criminal Screening (Annex 1)
2. Intelligence Gathering (Annex 2)
3. Referrals for Investigation and Prosecution (Annex 3)

Each area is examined for risk in relation to the collection, use, disclosure, retention and disposition of personal information.

5.1.1 Criminal Screening (Annex 1)

The screening annex contains provisions for both systematic and case by case vetting of permanent and temporary resident applicants, refugee claimants and citizenship applicants against RCMP criminal indices (CPIC and other law enforcement databases). Personal information provided by CIC for the purposes of screening includes both biographic and biometric (fingerprints) information. In the context of screening, the RCMP provides a service to CIC by providing screening results to support admissibility or eligibility determinations under IRPA or the Citizenship Act. This information could either be criminal record or criminal intelligence information. For refugee claimants, it also includes searches of possible previous claims under another identity.

The use of CIC screening information is subject to the following provisions set out in the draft screening annex:

> 4.3 The personal information provided to the RCMP, by CIC, for the purpose of carrying out screening function may only be used for the purposes of screening as outlined in this annex. The personal information may be used for other purposes only where permissible by law.
>
> 5.1 CIC and the RCMP will jointly develop screening guidelines as may be necessary with respect to the various lines of business where CIC sends requests to the RCMP for screening purposes under this annex.
>
> 6. Unless otherwise provided by law, personal information covered in this annex will not be used, disclosed or retained for purposes other than for the purpose for which it was collected.

The annex is intended to be principles based, with the implementation of screening guidelines where deemed necessary in order to provide additional guidance, instruction or clarification. Many of the current screening programs are already detailed in CIC manuals. Annex "A" details each screening program including the personal information provided, legislative authority, policy/procedural references, and screening results.

During the MOU consultation process, it became clear that certain aspects of the screening annex raise potential privacy questions in terms of access, use and disclosure of personal information. An in-depth

analysis of the screening process is provided in section 5.2 below. Risks and mitigation strategies are provided in section 6.

5.1.2 Intelligence Gathering (Annex 2)

The two organizations will share intelligence and other information relating to citizenship fraud, illegal migration movements, people smuggling, people trafficking and trafficking trends, fraudulent travel and identity document analysis, national security concerns, public security concerns, organized crime, money laundering, modern war crimes, crimes against humanity, genocide, terrorism, espionage and subversion.

Any exchanges of information under this annex must relate to a lawful investigation, the administration and enforcement of immigration laws, including the determination of admissibility, or the administration and enforcement of citizenship laws.

It is to be noted that the CBSA holds the principal intelligence gathering responsibility for IRPA. In turn, the RCMP covers intelligence responsibilities related to the Citizenship Act. Therefore the bulk of information exchanged with the RCMP under this annex will relate to citizenship. CIC is a consumer of intelligence products and information. It is not a producer of intelligence. Much of the information shared under this annex is non-personal in nature: trend information, risk profiles, country analysis, travel document abuse.

Privacy risk was assessed in terms of this annex, and no risk was identified. Exchanges under this annex are limited to the administration and enforcement of IRPA and the Citizenship Act. Exchanges are not systematic, but are case by case and information for the most part is depersonalized. Any cases originating from CIC which involve the exchange of personal information, would relate to a referral under the investigations annex (see next section). There are no new provisions for sharing in this annex; it is existing and ongoing business.

5.1.3 Referrals for Investigation and Prosecution (Annex 3)

This annex relates to the referral of cases to the RCMP for investigation and prosecution. It also includes provision for the referral of cases involving employee malfeasance. This annex supports the RCMP law enforcement mandate to investigate and refer for prosecution individuals who are alleged to have committed offences under IRPA or the Citizenship Act. CIC officers have a duty to apprise the RCMP of alleged offences and, subject to the Privacy Act provisions, to provide personal information. This annex reflects the ongoing and existing business and mandates of the two organizations.

It is to be noted that in most instances of exchanges under this annex, the CIC administrative process would be closely related to the law enforcement process (for instance misrepresentation or fraud in the citizenship process being addressed as both a ground of refusal and as an offence under the Citizenship Act), thus minimizing the risk of irrelevant information being passed to the RCMP. Exchanges in this respect are within the provisions of consistent use. Where the RCMP seeks personal information from CIC, either with respect to an alleged offence under IRPA or the Citizenship Act, it can also avail itself of the provisions of subsection 8(2)(e) of the Privacy Act, and make a written request for personal information for "the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation".

Privacy risk was examined in the context of this annex, and given the reasoning outlined above, no risk was identified.

5.2 Questionnaire A: RCMP Criminal Screening (Federal Programs and Services)

Given that risk has been identified in the exchange of personal information in the criminal screening process, the following detailed analysis of each of the principles of the Privacy Act has been completed.

Privacy Act **Principle 1: Accountability for Personal Information**

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
1.1 Has responsibility for the PIA been assigned? Please indicate in the details column the name and position of the person responsible.	**X**			John Kent, OMC Branch
1.2 Has the custody and control of personal information been determined?	**X**			Deputy Minister CIC Commissioner RCMP
1.3 Has the accountability of the program custodian of personal information been documented?	**X**			CIC ATIP Policies/Practices RCMP ATIP Policies/Practices Also documented in the MOU
1.4 Are the performance requirements of the custodian set out in a measurable way and subject to performance and compliance reviews?	**X**			Standard CIC and RCMP Audit and Evaluation Practices
1.5 Are third parties including the private sector involved in the custody or control of the personal information?	**X**			CBSA collects fingerprints in certain instances from refugee claimants CBSA coordinates the information exchange on TRV screening
1.6 If third parties or private sector parties are involved, do you have an agreement in place that establishes privacy requirements?	**X**			CIC-CBSA MOU

Questions For Analysis		Yes	No	N/D or N/A	Provide Details
1.7	If yes to 1.5, are the requirements of the *Personal Information Protection and Electronic Documents Act* applicable if the proposal involves the private sector?		**X**		
1.8	Will the department be provided with the results of regularly scheduled audits and compliance checks on the privacy requirements of all involved parties?	**X**			Internal audit provisions are established in the governing MOU (section 7.1)
1.9	Are the requirements for the Treasury Board *Policy on Privacy and Data Protection* being followed?	**X**			
1.10	Are there any requirements in program legislation or policies on the management of personal information that affect the proposal?		**X**		

Discussion Points: **No risks identified**.

Privacy Act Principle 2: Collection of Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
2.1 What is your authority to collect personal information? Please indicate the authority. If there is no authority, please consult with your legal advisor to determine if there is authority to proceed.	X			Section 4 Department of Citizenship and Immigration Sections 15 and 16 IRPA Section 22 Citizenship Act
2.2 Is the personal information collected directly related to an operating program or activity? s. 4	X			
2.3 Is personal information being collected directly from the individual? s. 5(1) If no, why not?		X		Initial screening information is direct from the individual Where positive match is made, personal information (criminal record for instance) will be from law enforcement databases accessible to the RCMP
2 4 Have the purposes for which the personal information is collected been documented? If yes, provide specifics. s. 4	X			Reference application form – excerpt attached. The relevant PIB also contain provision for sharing information with the RCMP.
2.5 Is all the personal information collected necessary to the operating program or activity?	X			To determine admissibility under IRPA or eligibility under the Citizenship Act
2.6 Is there notice at the collection stage that identifies the specific purposes for the collection, the authority for doing so and the individual serving as official contact? s. 5(2)	X			Yes, as part of the application form. Excerpt attached.
2.7 Is the notice associated with the collection of personal information available and consistent across all mediums of collection? s. 5(2)	X			

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
2.8 Are secondary uses contemplated for the information collected? s. 7 If yes, describe them in the details column.				Area of risk under review - law enforcement access to CIC client fingerprints and biographic information held by the RCMP; providing personal information to law enforcement agencies in Canada. Current practices are now under review to ensure they are within the provisions of "consistent use".
2.9 If personal information is to be used or disclosed for a secondary purpose not previously identified, is consent required? s. 7 & 8	**X**			
2.10 If consent is not required for secondary purpose use or disclosure, is there authority for the use or disclosure? s. 7 & 8		**X**		
2.11 Is information anonymized when used for planning, forecasting and/or evaluation purposes?	**X**			CIC follows proper research and evaluation protocols
2.12 Is personal information collected from a public database?		**X**		
2.13 Will quality assurance or security activities result in the collection of additional personal information?		**X**		
2.14 Does the program or activity involve the collection through a common client identifier? If yes, provide details about the identifier.	**X**			CIC client identifier

Discussion Points:

2.8: Identified risk: 1) Law enforcement <u>use</u> of CIC client fingerprints and related biographic information; and 2) Law enforcement <u>access</u> to CIC client biographic information. Areas of risk under review to ensure compliance with the Privacy Act.

Privacy Act Principle 3: Consent

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
3.1 Is consent obtained directly from the individual? If not, why not?	**X**			All immigration forms have consent provisions. The citizenship application form does not have consent for assessing eligibility. We have alerted our Citizenship program to address this issue.
3.2 How is consent obtained?	**X**			Application Form
3.3 Does consent require a positive action by an individual rather than being assumed as a default? s. 5, 7 & 8	**X**			Signature on form
3.4 If yes to 3.1 is the consent clear and unambiguous?	**X**			
3.5 If consent is sought, is the form of consent likely to stimulate negative reaction (for example, opt-in or -out)?		**X**		
3.6 Can an individual refuse to consent to the collection or use of personal information for a secondary purpose, unless required by law?		**X**		There is no opt out clause. Consent relates to the primary purpose only – assessing admissibility or eligibility.
3.7 Would the refusal of an individual to consent to the collection or use of personal information for a secondary purpose disrupt the level of program service provided to the individual?			**X**	Applicant can't refuse consent
3.8 Are standards and mechanisms in place to ensure that the individual has capacity to give consent? s. 77(1)(m)	**X**			Standard CIC practices
3.9 Are standards and mechanisms in place to ensure the recognition of persons authorized to make decisions on behalf of others (e.g. a minor or incapacitated person)? If not why not? s. 77(1)(m)	**X**			Standard CIC practices

Discussion Points: **No risk identified.**

Privacy Act Principle 4: Use of Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
4.1 What is your authority to use personal information? Please indicate the authority. If there is no authority please consult your legal advisor to determine the authority to proceed with the proposal.	**X**			Section 15 and 16 IRPA Section 22 Citizenship Act Section 4 Department of Citizenship and Immigration Act (DCIA) Section 8(1) Privacy Act
4.2 Is personal information used exclusively for the purpose for which the information was obtained or compiled? s. 7 (a)				Risk area under review. Law enforcement use to CIC client fingerprints and biographic information. Currently reviewing practices to ensure they are within the provisions of consistent use: see section 2.8.
4.3 Are the uses of the information limited to what a reasonable person would consider appropriate in the circumstances?				Area of risk under review. See section 2.8
4.4 Is personal information used for a purpose for which the information may be disclosed to the program by another institution? s. 7 (b)	**X**			RCMP and Law Enforcement Screening Process
4.5 Are personal identifiers, such as a social insurance number, used for the purposes of linking across multiple databases?	**X**			CIC Client Identifier Number
4.6 Where data matching, is it consistent with the stated purposes for which the personal information is collected?			**X**	
4.7 Does the data matching activity require a notification to the Privacy Commissioner?			**X**	
4.8 Is there an activity log attached to the personal information record to record uses not in the Index of Personal Information Banks? s. 9(1)?			**ND**	

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
4.9 Is personal information used for a consistent purpose that is not identified in a personal information bank? s. 9(4)		X		CIC personal information banks outline various consistent uses

Discussion Points:

Risk Identified: 4.2, 4.3

Privacy Act Principle 5: Disclosure and Disposition of Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
5.1 Is personal information disclosed with the consent of the individual? S. 8(1)		**X**		
5.2 If personal information is not disclosed with consent, has the specific authority for disclosure been identified? s. 8(2) If there is no authority to disclose personal information, please consult your departmental legal advisor.	**X**			s. 8(2)(a) Privacy Act
5.3 Are personal identifiers, such as a social insurance number, disclosed?	**X**			Yes, includes both biographic and biometric (fingerprints). See appendix A
5.4 Is the personal information to be disclosed limited to the purpose of disclosure?				CIC-RCMP: limited to purpose of disclosure RCMP-3rd party police agencies: area of risk – latent and other fingerprint matches. Biographic information. See 2.4
5.5 Is personal information disclosed for a purpose that is not identified in a personal information bank? s. 9(4) If yes, what is the method planned for disposal?		**X**		CIC Personal Information Banks outline various consistent uses
5.6 Will personal information be processed, disclosed or retained outside of Canada?	**X**			May be collected outside Canada but processed and retained in Canada
5.7 Is there an activity log attached to the personal information record to record the purposes of disclosure not listed in the Index of Personal Information Banks? s. 9(1)?	**X**			Standard CIC practices
5.8 Is the personal information scheduled for retention and disposition? s. 6(1) & (3) If yes, identify where in details column.		**X**		There is no CIC R&D schedule in place for fingerprints retained by the RCMP.

Discussion Points: **Risk Identified: 5.4, 5.5**

5.8: CIC has identified a need to review current R&D schedules for all lines of business. This is an issue that will need to be addressed as part of a larger Departmental strategy to update existing R&D schedules. Consequently, the specific requirements for R&D schedules relating to the RCMP MOU are considered out of scope of this review.

Privacy Act Principle 6: Accuracy of Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
6.1 Will steps be taken to ensure that the personal information is accurate, complete and up-to-date? s. 6(2)	**X**			Standard CIC practices RCMP ATIP Policies/Practices
6.2 Does the record of personal information indicate the date of last information update?	**X**			Above
6.3 Is a record kept of the source of the information used to make changes?	**X**			Above
6.4 Where applicable, is there a procedure, automatically or at the request of an individual, to provide notices of correction to third parties to whom personal information has been previously disclosed? S. 12(2)(c)	**X**			Above
6.5 Is there a record kept with respect of requests for a review of errors or omissions & corrections or decisions not to correct? s. 12(2)(b)	**X**			Above
6.6 Is there a clearly defined process by which an individual may access, assess and discuss or dispute the accuracy of the record? Please briefly describe the steps.	**X**			Above

Discussion Points: **No risk identified.**

Privacy Act Principle 7: Safeguarding Personal Information

Questions For Analysis		Yes	No	N/D or N/A	Provide Details
7.1	Has a Threat and Risk Assessment been completed?			**N/A**	Outside of scope
7.2	Have security procedures for the collection, transmission, storage and disposal of personal information, and access to it, been documented?	**X**			Standard RCMP practices Specific provisions ensuring proper handling of information also established in the MOU and annexes
7.3	Are program and information technology staff trained in the requirements for protecting personal information and are they aware of the relevant policies regarding breaches of security or confidentiality?	**X**			RCMP and CIC practices and procedures
7.4	Are there controls in place for any process to grant authorization to modify (add, change or delete) personal information from records?	**X**			RCMP procedures/audit and security
7.5	Is the system designed so that access and changes to personal information can be audited by date and user identification?	**X**			Split responsibility. RCMP and CIC practices and procedure
7.6	Are user accounts, access rights and security authorizations controlled by a system or record management process?	**X**			RCMP and CIC practices and procedures.
7.7	Are access rights only provided to users on a "need to know basis" consistent with the stated purposes for which the personal information was collected? s. 5(2)	**X**			RCMP Practices. Law enforcement access to CIC client biographic information previously identified as risk.
7.8	Are security measures commensurate with the sensitivity of the information recorded?	**X**			CIC and RCMP Practices and Procedures

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
7.9 Are there contingency plans and documented procedures in place to identify and respond to security breaches or disclosures of personal information in error?	**X**			RCMP ATIP Policies/Practices
7.10 Are there documented procedures in place to communicate security violations to the data subject, law enforcement authorities and relevant program managers?	**X**			RCMP ATIP Policies/Practices
7.11 Is there a plan for quality assurance and audit programs to assess the ongoing state of the safeguards applicable to the system?	**X**			RCMP ATIP Policies/Practices

Discussion Points: **Risk Identified: 7.7**

RCMP procedures and practices for safeguarding personal information often set the standard for government.

Privacy Act Principle 8: Openness

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
8.1 Describe how the results of any privacy impact assessment or audit will be made available to the public.	**X**			Summary to be posted on-line
8.2 Are policies and practices relating to the proposal's management and handling of personal information available to the public?	**X**			The RCMP MOU and Annexes will be posted on-line.
8.3 Is there a communications plan to explain to the public how personal information will be managed and protected?		**X**		
8.4 Is there a clearly defined and easy process for individuals to access such information and/or communicate with appropriate individuals with respect to policies and practices relating to management and protection of personal information?	**X**			CIC ATIP process RCMP ATIP Process
8.5 Where appropriate, have key stakeholders been provided with an opportunity to comment on the privacy protection implications of the proposal?	**X**			Yes, CBSA informed. OPC informed.
8.6 Where appropriate, will public consultation take place on the privacy implications of the proposal?		**X**		
8.7 Has the personal information been included in a personal information bank? s. 10	**X**			

Discussion Points: **No risk identified.**

Privacy Act Principle 9: Individual's Access to Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
9.1 Is the system designed to ensure that an individual can have access to his/her personal information including all other programs or applications that have received copies of the information? s. 12(10)	X			CIC ATIP procedure RCMP ATIP procedures
9.2 Is the system designed to ensure that an individual has been notified that a correction to his/her information has been made?	X			above
9.3 Are all custodians and participants aware of an individual's right of access and the complaint process?	X			above
9.4 Are there documented procedures developed or planned on how to initiate privacy requests or requests for the correction of personal information? s. 12 (2)	X			above
9.5 Has consideration been given to providing individuals "routine" access to their personal information?		X		ATIP process to be followed
9.6 Are individuals provided with access to their personal information in the official language of choice? s. 17(2)	X			CIC and RCMP ATIP procedures
9.7 If appropriate, are individuals provided with access to their personal information in alternative format? s. 17(3)	X			above

Discussion Points: **CIC and RCMP ATIP Practices and Procedures. No risk identified.**

Privacy Act Principle 10: Challenging Compliance

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
10.1 Are the complaint procedures for the proposed program or service consistent with legislated requirements? s. 29-35	**X**			CIC ATIP process RCMP ATIP process
10.2 To improve information management practices and standards, has a procedure been established to log and periodically review the nature, frequency and resolution of complaints?	**X**			above
10.3 Are there oversight and review mechanisms implemented or available to ensure accountability?	**X**			above
10.4 Have oversight agencies, including the Office of the Privacy Commissioner, issued reports or opinions on issues that would be relevant to the proposal? If yes, please provide a summary of the above in the details column and append to final report.		**X**		Not at this time

Discussion Points: **No risk identified.**

6. Privacy Risk Management Plan

6.1 Privacy Risk and Mitigation

6.1.1 Law Enforcement Access to and Use of CIC Client Personal Information

There are two privacy risks associated to criminal screening under the admissibility provisions of IRPA. To fully appreciate these risks, it is important to first set out the broader context in which they take place.

Criminal Screening in Context

C&I Officers perform a critical role: they must ensure all applicants for immigration and citizenship meet admissibility and eligibility requirements under IRPA and the Citizenship Act. Specific legislative provisions address criminal and security requirements with the objective of ensuring the safety and protection of Canada. (section 3 IRPA; section 22 Citizenship Act). With respect to admissibility, it is not a static process, rather it is a continuum where new or additional information can affect admissibility decisions. C&I Officers must have the most up to date and accurate information available in order to meet their responsibilities. It bears keeping in mind that in a world of growing criminal enterprise and sophistication, it is essential that C&I Officers have the most advanced means and tools at their disposal to identify and collect new and relevant admissibility information.

The RCMP, as Canada's national police force, is a key partner in supporting CIC in meeting its admissibility responsibilities. The RCMP is an entrenched part of the larger Canadian law enforcement information network. This includes various system interfaces with federal, provincial and municipal level police agencies. The RCMP administers the national CPIC criminal information system, and has access to the multitude of police and intelligence databases of the larger policing community. It is in this respect that CIC has a critical interest: to ensure a robust screening program, CIC depends on the RCMP's ability to leverage these information systems. Information relevant to admissibility could include information arising from a criminal investigation, criminal intelligence, criminal charges and/or convictions. In order to identify and collect this information, it entails in the first instance that CIC share personal information of its client base. It is in this respect that potential privacy risks arise.

Risk Assessment

There are two general types of RCMP criminal screening processes:

1) Biometric Screening: fingerprints which includes associated limited biographic information such as name and date of birth; checked against the RCMP national fingerprint database (AFIS)
2) Biographic Screening: name, date of birth, gender (without fingerprints) and related personal background information; checked against RCMP and law enforcement databases

With respect to biometric information, fingerprint screening is currently conducted systematically for refugee claimants (but will also include temporary resident applicants starting in 2013). Biographic screening is conducted either systematically or on a case-by–case basis depending on the screening category. For temporary resident visa (TRV) applicants, it is case by case, and is based on country risk indicators. The RCMP provides screening results in order to assist CIC officers in making admissibility decisions under IRPA. This initial screening decision is conducted within the provisions of consistent use. The RCMP then retains the biographic and biometric information in various databases.

There are two circumstances where risk arises with respect to access and use of CIC screening information.

1) Fingerprints Submitted by Law Enforcement Agencies Matching against CIC Fingerprints and Potential for Secondary Use

   Issue: Following an initial RCMP screening decision, a fingerprint submitted by a law enforcement agency can match to a CIC client fingerprint stored in the RCMP national fingerprint database. This could result in the disclosure of CIC client personal information to the law enforcement agency. There is a risk that disclosures of this type may not always be authorized.

   Analysis: Disclosures occurring from the above described scenario are authorized when the disclosure is related to a consistent use. The disclosure could be consistent use when the fingerprints submitted by the law enforcement agency were taken during an arrest or charge, because of the potential criminal activity involved and its relevance to an admissibility determination. There may also be instances a fingerprint match indicates misrepresentation because the biographic information associated with the fingerprint does not match to that which was submitted by the law enforcement agency. In this scenario, and depending on the information under the control of the law enforcement agency, CIC could be collecting new criminal information and potential misrepresentation information relevant to the admissibility determination. This would represent an extension of the screening process. The level of privacy risk is deemed negligible so long as CIC is potentially receiving relevant information back.

   However, there are other instances when a law enforcement agency submits a fingerprint for searching in the national fingerprint repository. These include latent (unidentified) fingerprints, fingerprints taken from victims of crimes, witnesses, or those suffering amnesia, etc. Disclosures of personal information resulting from these types of fingerprint matches would not be deemed consistent use, and as such, the privacy risks are higher. There are specific concerns when the match is made to a latent fingerprint. While it is clearly within the realm of possibility that the latent fingerprint match could alert CIC to new and relevant information such as the criminal investigation of a CIC client, it is also very possible that the information has nothing to do with a criminal activity of the individual concerned, but instead relates to the identification of a witness, bystander, victim, cadaver, or other non-criminal scenario. These are circumstances where the law enforcement agency is seeking personal information solely to assist in its investigation. While there may be a broader public interest in identifying individuals in these situations, it represents a change in purpose from IRPA administration to criminal/law enforcement and is therefore not consistent use.

   In summary, the sharing of CIC client fingerprints and related biographic information with law enforcement agencies is generally within the provisions of consistent use. CIC has an interest to ensure that its clients are properly identified in law enforcement processes and that any relevant information affecting a client's admissibility (charges, arrests, criminal intelligence, conflicting identity information, criminal convictions) is brought to its attention. This necessitates the sharing of CIC client personal information. However, due to the variety of "non consistent use" scenarios specific to latent fingerprint matches, the privacy risk is deemed to be significant.

   Risk Mitigation: CIC will be proposing legislative and regulatory authorities authorizing the RCMP to use and disclose CIC client biometric information for law enforcement (secondary)

purposes. Once approved and in force, these authorities will mitigate the risks associated with disclosure of information resulting from latent fingerprint matches. These authorities are planned to be in place in 2013.

In the meantime, CIC is currently reviewing its policy and practices with a view to establishing interim measures to address the risks related to disclosure of biometric and other personal information in cases of latent fingerprint matches. Once finalized, CIC will provide the OPC with its new policy instructions.

2) Access to Biographic Personal Information of Temporary Resident Visa Applicants

Issue: CIC provides the RCMP with biographical and other detailed personal background information (employment history, residence history, family etc) in order for the RCMP to conduct background checks of selected TRV applicants based on country risk profiles. These checks are conducted to determine admissibility under sections 36 and 37 of IRPA (criminality and organized crime provisions). This part of the screening process is coordinated through the National Security Screening Division of CBSA on behalf of CIC. The checks are within the provisions of consistent use. The RCMP retains the information in its national database (PROS) for a period of 10 years. During this period, law enforcement agencies in Canada have access to the personal information stored in the database. The risk is that law enforcement access may lead to the sharing of CIC personal information outside of the provisions of consistent use or without other lawful authority.

Analysis: There are various scenarios where law enforcement agencies in Canada could match biographic information of an individual under police investigation to a CIC client in the RCMP database. It will depend on the purpose of access as to whether it is consistent use. If the agency in making the match is providing updated criminal information (criminal associations for instance) relevant to the CIC admissibility determination, it would be consistent use. So long as relevant information is provided to CIC in the exchange, it would reflect a continuity of the screening process. However, there could be a multitude of scenarios which are not consistent use. The concern is that without any control or check on access to the RCMP database, there is no way to ensure the information exchange is appropriate and within the provisions of consistent use. This represents a significant privacy risk.

Risk Mitigation:

CIC is currently reviewing practices in relation to law enforcement access to CIC client biographic information held in the RCMP database. The review will examine potential imposition of controls and other safeguards towards ensuring consistent use of CIC screening information. The review will require internal and external consultations as well as an assessment of any operational implications. CIC anticipates a 6 month period to complete the review. Once finalized, CIC will provide the OPC with its new policy instructions.

6.2 Summary Table

Meaning of Risk Levels:
Low: There is a possibility that the risk will materialize but there are mitigating factors.
Medium: There is a strong possibility that the risk will materialize if no corrective measures are taken.
High: There is a near certainty that the risk will materialize if no corrective measures are taken.

Element	Nature of Risks	Level of Risks			Comments	Mitigating Mechanisms
		Low	Medium	High		
Latent Fingerprint Matches to CIC Clients	Question of Consistent Use and Lawful Authority		XX		CIC is currently consulting on interim measures.	1) Legislative Authority 2) Interim Measures and Safeguards
Law Enforcement Access to CIC Biographical information	Question of Consistent Use		XX		CIC is currently consulting on interim measures	1) Safeguards and Controls on access